Clarifying Broad Hacking Statutes

Gudmundsdóttir, Helena Lybæk

DOI (link to publication from Publisher):
10.5278/vbn.phd.socsci.00056

Publication date:
2015

Document Version
Publisher's PDF, also known as Version of record

CLARIFYING BROAD HACKING STATUTES

BY
Helena Lybæk Guðmundsdóttir

DISSERTATION SUBMITTED 2015

AALBORG UNIVERSITY
DENMARK

Aalborg University

Clarifying Broad Hacking Statutes

Helena Lybæk Guðmundsdóttir
9-15-2015

Dissertation submitted: November 2015

PhD supervisor: Professor Lars Bo Langsted
Aalborg University

PhD committee: Professor Søren Sandfeld Jakobsen
Aalborg University

Professor Inger Marie Sunde
Politihøgskolen i Oslo

Professor Thomas Elholm
The University of Southern Denmark

PhD Series: Faculty of Social Sciences, Aalborg University

ISSN (online): 2246-1256
ISBN (online): 978-87-7112-839-0

Published by:
Aalborg University Press
Skjernvej 4A, 2nd floor
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Rosendahls, 2016

1 INTRODUCTION

1.1 The problem

The broadly worded Danish criminal code § 263(2), popularly known as "the hacking provision", has been around for thirty years, and yet surprisingly little is known about its scope and how it might be interpreted and construed in practice. When the provision entered into force on 1 July 1985, the only other country in the world that had enacted a dedicated computer crime statute was the United States.[1] US courts have extensive experience with computer crime compared to Danish courts that have seen relatively few computer crime cases. The Danish hacking provision has therefore seen little action over the years and its scope is largely unclear; and with respect to the courts' construction of the provision in one of the few cases that exist, the construction was criticized by a commentator.[2]

Under the Council of Europe's Convention on Cybercrime, both the US and Denmark, as well as other states, have undertaken international obligations to achieve some minimum harmonization of national substantive criminal law by criminalizing certain basic types of cybercrime. During the negotiation of the Convention, the US had considerable influence on the drafting process, and the Convention, according to the US Department of Justice, essentially reflects existing US law, which is presumably supported by Congress's statement that no legislative implementation of the Convention was required to meet the US' obligations. The Danish sentiment was the same in that no amendments to substantive criminal law were considered required. Even though Denmark and the US were among the first countries in the world to enact computer crime legislation thirty years ago, it is still oddly unclear what conduct is being criminalized through the broadly phrased illegal access statutes. Whereas the US courts, as mentioned above, have gained some experience with applying the CFAA, and case law, thus, provides some insights into how such a statute might be

[1] Bent Carlsen and Michael Elmer: Datakriminalitet (1986), Juristen, p. 297. The article mentions only the existence of US state laws, but the federal Computer Fraud and Abuse Act's (CFAA) predecessor, the Counterfeit Access Device and Computer Fraud and Abuse Act (CADCFAA), was already in force in 1984 although it was very narrow in scope compared to the CFAA. In the US, computer crime bills had been introduced into Congress on several occasions since the late 1970s, but their sponsors' pleas fell on deaf ears, as Congress ostensibly opined that current legislation was sufficient to address computer crimes. It was not until circa 1983, when 21 states had passed computer crime laws, after a number of high-profile hacks combined with Congress' awareness of the movie WarGames. See Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), p. 23

[2] See criticism of a Danish High Court's implicit rejection of a broad construction of "unauthorized" in Mads Bryde Andersen: IT-retten (2005), p. 746. The same commentator has criticized the decision in other publications as well. See e.g. Jørn Vestergaard & Flemming Balvig (ed.): Med lov…: Retsvidenskabelige betragtninger (1998), Mads Bryde Andersen: Overvågning af medarbejdere, pp. 59-60. The criticized decision, U 1996.979 Ø, is analyzed below in the chapter on authorization with respect to insiders.

applied, Danish courts have very little experience with the hacking provision, and very few decisions are available. The few decisions that are available concern rather typical "hacking" (use of hacking tools to circumvent security measures) and, as is rather typical for Danish courts, the reasoning for the decisions is scant.

The American Computer Fraud and Abuse Act, the CoE's Convention on Cybercrime, the Danish hacking provision (criminal code § 263), all state computer crime laws in the US, and so on, have in common two concepts that are the fundamental building blocks of every hacking statute; namely, the concepts of without authorization/right and access.[3] Thirty years ago computers were by no means widely owned by the public and were not integrated in everyday activities, and thus, there were by far fewer people with access to computers that could trigger criminal liability.

In 1985, the World Wide Web[4] had not yet been invented and browsers, HTTP[5], HTML[6], web servers and websites did not yet exist. Only five years later, in 1990, the commercial restriction on the use of the Internet was lifted.[7] As mentioned above, in 1985, the Danish committee on criminal law, observant of the development in the United States and considering the few cases of computer crime that had arisen in Denmark at that time, reviewed the Danish criminal code in order to assess whether it needed to be amended to cover computer crimes. It is important to keep in mind that the Committee's report and the Danish hacking provision[8] were written at a time that greatly differs from today in terms of the stage of technological advancement in computer science.

However, at that time computers were mostly not networked, and the Internet was not commercialized yet. A few large university networks and military networks were interconnected, but on a very small scale compared to today. (See e.g. map[9] of the mid-80s Internet below.)

[3] See Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, pp. 1615-1616
[4] Note that the Web and the Internet are terms often erroneously used synonymously. Whereas the Internet is the "network of networks", the Web is one of the "services" that run over the Internet.
[5] HyperText Transfer Protocol
[6] HyperText Markup Language
[7] Pieter Hintjens: Culture & Empire (2013), p. 30
[8] And so were the US senate reports regarding the US federal computer crime provisions that date back to 1984.
[9] Retrieved from https://en.wikipedia.org/wiki/File:InetCirca85.jpg on 05 January 2015. Image is public domain.

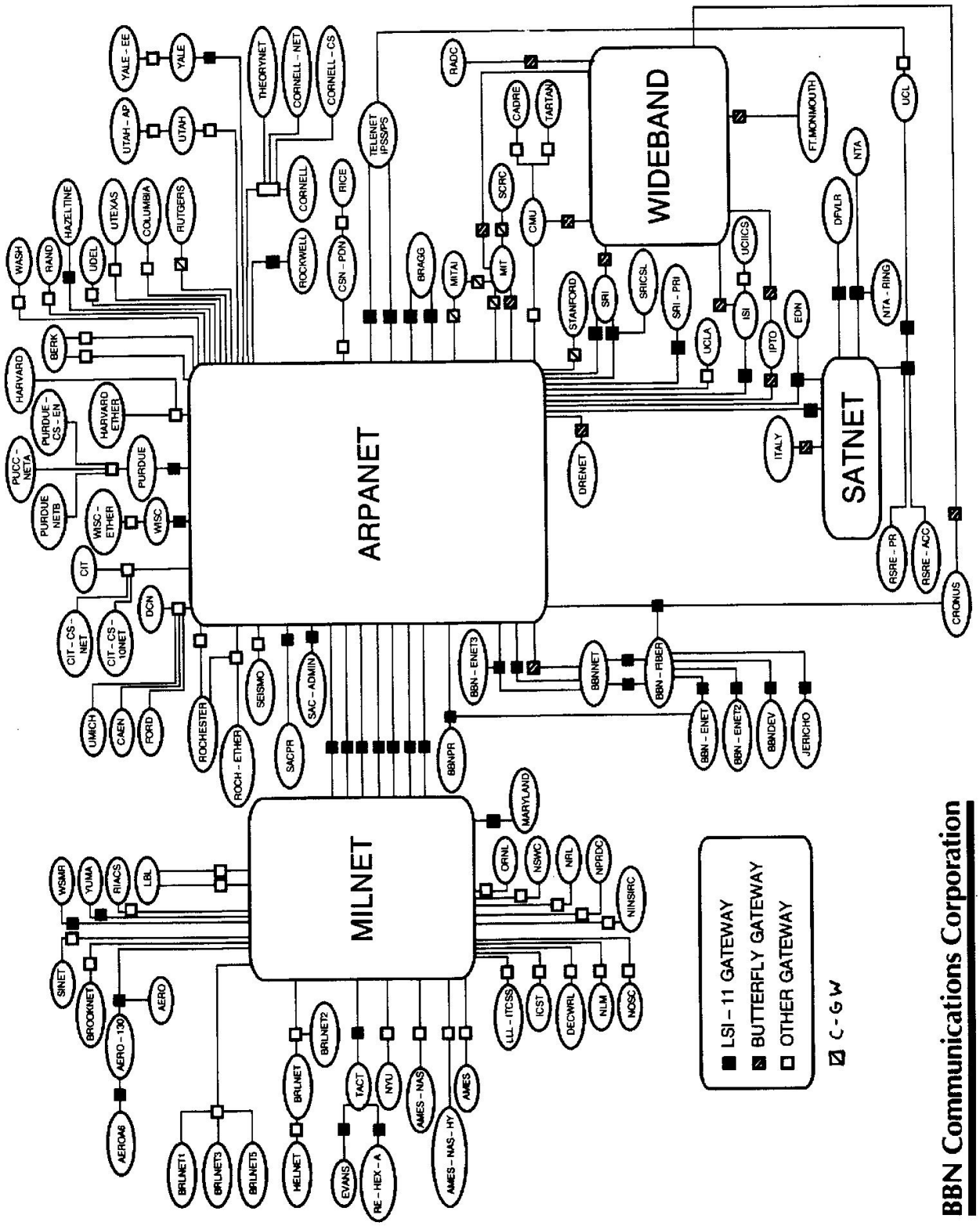


Image 1 A map of the entire Internet in late 1985 to early 1986 - Work of the US Department of Defense

In 1985, it was much easier to determine whether a person had accessed information or programs. Accessing a computer, and the information and programs it contained, would either occur by physically sitting by the computer and opening files, using programs and so on or establishing a remote connection to another computer much like today but with considerably more effort, skill and cost and therefore of limited direct use for the average person. In order to establish a remote connection, one would generally have to have knowledge of the phone number associated with the modem connected to the computer one wanted to access, and one would generally need a password to establish the connection. Today we access information and programs hundreds or thousands of

times a day[10], if not far more often, without much or any knowledge of what takes place behind the scenes – most of the material being publicly accessible to anyone. The user is much less, if at all, aware of the underlying mechanics of established connections, accesses granted or denied, and so on, unless explicitly presented with access restrictions. Out of the five[11] cybercrime legislations addressed, albeit to varying degrees, in this dissertation, only the drafters of the Convention on Cybercrime[12], took the increased interconnectivity and the invention of the World Wide Web, from the point of the user, into consideration when addressing unauthorized access; however, they only did so through the explanatory report adopted alongside the Convention.

However, the scope of hacking statutes was not problem free even when Internet access was not an everyday commodity and there was no world wide web. The statutes were still unclear in terms of what triggered criminal liability when employees misused computers (typically for purposes that the employer disliked), and that lack of clarity still persists in form of disagreement between courts, commentators and others. The only thing we can seemingly agree on is that the typical idea of a hacker who breaks into computers by exploiting vulnerabilities and those accessing by the guessing other people's passwords have committed the crime of unauthorized access. However, the statutory language does by no means stop there. The term "without authorization/right" is sufficiently vague to let aggressive prosecutors and plaintiffs be creative. Combined with the fact that the objective element of the crime (access to a computer or information and programs) is met by most people hundreds of times a day, one need only find one out of those hundreds of times where authorization could be called into question. Thus, a number of competing approaches to construing "authorization" appear; prosecution and plaintiff theories typically being very broad and defendants' theories narrower. For example, in one jurisdiction in the US, if an authorized employee accesses a computer or information with a disloyal motive, that person will cease to be an agent of the employer and automatically loses their authorization at the time of the access. In other jurisdictions, access may ***become*** unauthorized, if the subsequent use of information or the service provided is an intentional breach of contract (including intentional breaches of terms of use and

[10] Particularly, if every dynamic element on a website is counted. We access and retrieve information from third parties' computers without necessarily being aware of doing so.

[11] The CoE Convention on Cybercrime, the Council's Framework Decision 2005/222/JHA on attacks against information systems, Directive 2013/40/EU on attacks against information systems, the Danish criminal code § 263(2), and 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act). U.S.C. is short for United States Code.

[12] The Convention entered into force on January 1st 2007 in the US and on October 1st 2005 in Denmark. Currently, 42 countries have ratified the Convention and 11 countries have signed but not ratified. *See* Council of Europe, Chart of Signatures and Ratification, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG accessed July 1st 2014

service on websites). Many of us have children that signed up for a Facebook account before they turned thirteen years old. Those of us who read the terms of service intentionally breached the terms of service by aiding our children in creating an account. Those who use Facebook are similarly contractually bound to keep their information up to date. Of course, most courts would think twice before basing a criminal conviction on breach of such terms, but the statutory language does not exclude those situations from criminal liability, and thus we find ourselves at the mercy of our prosecutors and courts. This not only raises the question of whether hacking statutes should perhaps be a bit more specific as to what they criminalize, but it also raises the question how courts determine what authorization means when they evaluate whether access was without authorization.[13]

Thus, the problem is that unauthorized access statutes use broad terms such as "access", and "computer" or "information" that essentially includes any interaction with technology and information. The broad language, which is itself ambiguous in that it leaves doubt as to what is meant by "access" (which again comes in broad and narrow flavors), is then meant to be modified by the rather unclear concept of "without authorization/right". That is then further complicated by technology, since people often need to rely on analogies to describe the facts, and the choice of analogy can direct the application of the legal rule. For example, it could be relevant when determining if access was unauthorized, whether some software or code could be described as a technical barrier to access, the circumvention of which would make it clear that access was unauthorized and thus criminal; or whether a sequence of letters or numbers used in a certain context is akin to a password even though they do not fit our conventional ideas of passwords. For example, Netflix directs Danish customers to the Danish version of Netflix, because their IP address indicates they are in Denmark. Does it constitute a circumvention of a technical barrier to use a VPN service to access other regional versions of Netflix? That is, describing the facts in a clear and concise manner in unauthorized access cases can be hard and may itself be subject to interpretation (e.g. what a snippet of code is meant to do compared to what people may perceive it as doing). How you choose to describe the technology becomes relevant to the application of the legal rule in that it

[13] In connection with the Convention on Cybercrime and the fact that it allows each party to decide the meaning of "without right", it has been remarked that lack of homogeneity with respect to the meaning of "unauthorized"/"without right" can create problems. See discussion paper by Lorenzo Picotti and Ivan Salvadori: National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices (2008), p. 12. Available on the Council of Europe's website at https://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf. Last visited on 13 September 2015.

can affect the outcome of the case. Thus, when hacking statutes are very broad and contain unclear terms themselves, the degree of uncertainty regarding e.g. the choice of analogies when describing technical facts again makes hacking statutes extremely versatile, because if some software or other code can be described as analogous to more conventional technical barriers, this directly affects the determination of whether access was unauthorized.

Although some degree of uncertainty is present in most legislation and unclear legal terms are nothing new, it is especially challenging when criminal liability may hinge on how code and its effects is interpreted and described; and there are often more than one ways to describe the functioning and effect of code.

This compounded lack of clarity leaves the courts in an unenviable position when they are confronted with cases outside the few examples most of us agree is certainly unauthorized access, such as guessing passwords to gain access to another person's account without their permission.

1.2 Research questions

How can "without authorization/right" be clarified through interpretation and construction?

What are the consequences of the various ways of interpreting "without authorization/right" with respect to the clarity and precision required of criminal statutes?

The answers to those questions are then meant to lead the way to finding a suitable approach to interpreting broadly phrased hacking statutes. The suitable approach must live up to the requirements of clarity and precision required of criminal law, in that it provides reasonable foreseeability to the regulated persons and does not allow or encourage arbitrary enforcement of the law.

1.3 Delimitation

There is no single definition of what cybercrime is. This dissertation focuses on illegal access crimes committed against computers. These are crimes that fall within the category of being attacks

against a computer, rather than merely being a manifestation of a traditional crime committed by use of a computer, e.g. fraud or content-related crimes such as copyright infringement. Equally excluded from the scope is procedural law and rules of evidence.

Illegal access crimes may encourage calling into play many areas of law though. However, for the purposes of this dissertation the main focus is criminal law and, to an extent, whether violations of other laws can or should trigger a violation of an illegal access provision. Examples of such other laws are data protection law, copyright law, trade secret law and contract law. These areas of law are not addressed in any detail, but are included to the extent that they are relevant to the particular question at hand. Thus, there will be no general or specific analysis of other areas of law than criminal law.

Furthermore, this dissertation is focused on the objective elements of the crime of illegal access, and is not concerned with subjective elements of the crime. For that reason, there will be no analysis or specific accounts of the meaning of such general principles of criminal law as intent, recklessness, attempt, aiding and abetting, and the likes. It is recognized that such principles have an effect on the extent of a criminal statute's scope, but the harmonization efforts made by e.g. the Convention on Cybercrime and EU cybercrime legislation were never aimed at harmonizing general principles of criminal law; only the objective elements of the crime. However, the lack of harmonization of general principles affects the degree of harmonization possible.

For good measure it should be noted that although criminological considerations are generally interesting, they fall outside the scope of this dissertation. Similarly, law and economics perspectives also fall outside the scope of this dissertation even though such analyses could be very interesting in the context of a property vs. liability inquiry, for example in terms of cases where US courts have given owners of public websites the right to exclude selectively certain persons from accessing their public websites (typically the exclusion of competitors who are seeking information to compete more efficiently, or exclusion of persons providing services that complement the owner's primary service). Such cases could also raise questions with respect to competition law, but this as well, falls outside the scope of this dissertation.

It would be interesting to examine the problem of vague hacking statutes in light of conduct protected by fundamental human rights, such as freedom of expression, including the right to seek out information. However, analyzing the meaning and extent of the scope of illegal access statutes is arguably a prerequisite for further research into how that scope then compares to and perhaps is

influenced by e.g. freedom of expression. Until the scope, or rather the possible scope, of illegal access statutes is documented, as this dissertation attempts to do, it is hard to say whether such a scope conflicts with freedom of expression or other protected conduct. The scope of those human rights would also require extensive and time consuming research and analysis. An analysis of the possible scope of hacking statutes in light of fundamental rights deserves more attention and detail than time allows, considering the considerable challenge involved solely with figuring out what should and should not trigger hacking statutes by drawing upon experiences of a foreign legal system.

With respect to foreign legal systems, the US law drawn upon in this dissertation is not intended to serve as a full-scale comparative analysis, but as inspiration and guidance with respect to experiences with applying very similar statutory language, which is also intended to implement the Convention on Cybercrime, in order to figure out an appropriate method of applying the Danish hacking provision whilst avoiding pitfalls that have led to unconstitutional applications of the federal hacking statute in the US (that might in the Danish context trigger a violation of article 7 ECHR) or interpretations and constructions that have sharply divided US federal courts as to the meaning and scope of the federal hacking statute. The result of these inquiries and analyses may in turn be transferrable to other jurisdictions using the same or similar statutory language, who also have discovered that the meaning of unauthorized access is not as unambiguous and largely unproblematic as originally thought. This problem is hardly one isolated to the US and Denmark, since close to fifty countries have ratified the Convention on Cybercrime and, thus, are obligated to criminalize illegal access even though it is unclear what illegal access really is when it comes to applying the law in practice. Arguably, such lack of clarity is not the best foundation for harmonization of substantive criminal law.

All in all, there are many aspects of hacking statutes that cannot be addressed within the confines of this dissertation that nonetheless deserve attention and research, because the problems are unlikely to go away on their own given the increasing interconnected-ness and computerization in most aspects of life.

1.4 Structure of the dissertation

Chapter 2 explains the problem of description as it relates to facts and the law. This dissertation does not as such focus on the particular variations in description of facts. That is primarily the role of evidentiary inquiries. However, the point must be made that in terms of computers and networks, facts can be viewed from different perspectives, forcing the legal practitioners to make choices between perspectives. The choice of perspective can then in turn decisively affect the process of applying the legal rule and may dictate different outcomes. A comparative perspective is introduced as an inspiration to solving the problems related to describing the meaning of the law. This comparative perspective, which is based on the extensive experience US courts have with interpreting and construing the federal hacking statute, does not stand alone, of course. The purpose of the comparative perspective is not to import US law, but to examine possible extents of a statute quite similar to the Danish provision, where both are intended to implement the Convention on Cybercrime. Furthermore, it may be possible to derive at least an analytical framework for determining when access is authorized without borrowing any the legal rules themselves. That way, the framework would provide a more methodical way of applying the Danish provision, or perhaps just explains the way Danish courts are already applying the hacking provision (because Danish courts do not provide extensive explanations of their interpretative approaches if such approaches were intentionally applied). A framework for applying the provision, and/or explaining the current application of the provision, would serve to further clarity and foreseeability of the provision's application.

Chapter 3 rather briefly introduces the sources of law that play a part in understanding unauthorized access provisions, along with a few secondary authorities associated with those sources. The chapter addresses what status the international sources have in the domestic legal systems (although strictly they are not necessarily sources of law, depending their status within the domestic legal systems). Furthermore, the chapter reveals that the Convention, EU cybercrime law, US law and Danish law are not drafted independently of each other, but it turns out that US law may have affected the drafting of the Convention, which in turn is the basis for EU cybercrime law. At the time the Danish hacking provision was enacted, only the US had computer crime laws. One of the earliest computer crime literature in Denmark also looked to US law to an extent[14], as well as US experience with computer crime law being mentioned in the committee report in which the Danish

[14] Vagn Greve: edb-strafferet (1986)

hacking provision was proposed. Of course, that does not mean that the Danish hacking provision or the Convention are directly based on US law, but it is natural when drafting a new law or convention to look around and see what others have done and consider their experiences.

Chapter 4 addresses interpretation and construction. These are vital processes to any legal professional, but they particularly important tools when applying broad and unclear provisions. The chapter also serves the purpose of providing the framework for the use of the sources of law (and a few secondary authorities) discussed in chapter 3. This is particularly needed in terms of figuring out to what degree international and EU sources can affect US and Danish domestic law. This is particularly interesting with respect to determining the possible degree of harmonization when the rules meant to be harmonized leave extensive room for vastly different approaches to interpretation and construction of those rules when implemented in domestic law.

Chapter 5 describes the meaning of nullum crimen sine lege principle. The purpose of the chapter is to reveal the extent of legal protection the principle provides, and discuss whether lack of clarity, vagueness or ambiguity inherent in statutory language using broad and general terms could conflict with the principle. Very open-ended criminal statutes may be convenient for the state, but less so for the citizens' ability to predict whether any given behavior is criminal or not.

Chapter 6 describes the history and purpose of the 2001 Convention, the criminalization therein, and how the Explanatory Report accompanying the Convention takes the advent of the Web and the commercialization of the Internet into consideration when describing the intended scope of the criminalization.

Chapter 7 concerns EU cybercrime legislation. The EU followed up with its own legislation, the Council's Framework Decision on attacks against information systems. Due to lack of will to renegotiate the Convention to adjust for modern day cybercrimes, the EU took legislative action in form of a directive in 2013, which repealed and replaced the older framework decision.

Chapter 8 addresses the Danish hacking provisions. The initial criminalization of computer crime in 1985, as well as the 2002 implementation of the Cybercrime Convention and the EU Framework Decision on attacks against information systems are covered in this chapter.

Chapter 9 discusses the US Federal hacking statute known as the Computer Fraud and Abuse Act (CFAA). The CFAA contains very similar language to the Danish legislation. Contrary to the Danish hacking provisions, there has been much more case law generated under the CFAA. This

US case law therefore provides a comparative perspective as to the possible reaches of a broadly worded hacking statute, since hacking statutes generally contain the same fundamental elements of the crime. This despite the seemingly much narrower intended scope of the statute.

Chapter 10 contains an analysis and discussion of the meaning of "access", and how it is or may be interpreted under the various hacking provisions. For example, the explanatory report adopt alongside the Convention provides a non-authoritative interpretation of access. It is therefore the goal of this chapter to figure out how "access" is interpreted and construed, and how that interpretation may affect the scope of hacking statutes and the role "without authorization/right" plays.

Chapter 11 contains an analysis and discussion of the meaning of authorization with respect to outsiders; that is, with respect to people who do not have special permission to access. These situations typically involve access to websites, where authorization to access is implied. The chapter thus also touches upon exclusion from access to public websites and cases where plaintiffs or the prosecution have claimed that access to information was unauthorized because it was not purposely made public, and that the defendant did or should have realized that. Because the hacking statutes are thirty years old, they do not take into account situations where access is authorized in absence of special permission such as is the case with public websites, and thus do not explicitly exclude e.g. access to public websites from their scope. Thus, the hacking statutes can provide for some surprising applications in that sense.

Chapter 12 addresses the application of hacking statutes to insiders. Their authorization is delegated specifically to them, and they have access to information that exceeds that which is accessible to the public or other insiders. Insiders are typically employees, since employees gain special access to their employers systems that is not available to those with no such relationship with the employer. Authorization with respect to insiders is a tricky issue, even though it was something that was specifically contemplated in legislative history.

Chapter 13 contains an article discussing the lack of qualitative limitation of the scope of the Danish Criminal Code's section 193. Section 193 prohibits causing massive disturbance of the functioning of a number of systems, including information systems. The article was published in the journal *Juristen* in July 2015.

Chapter 14 contains the conclusion and other final remarks. Whilst chapters 15 and 16 contain abstracts in Danish and English, respectively.

2 PERSPECTIVES ON THE PROBLEM

2.1 Problems with description

The problem with description concerns both problems with describing facts and problems with describing law and thus determining the legally relevant facts. The problem with describing the facts in context of computers can be said to be generally owed to inconsistent and unclear terminology in IT and the malleable functioning of computers, and thus the way of describing the function of computers and code. The problem with describing the law (i.e. its legal content, and thus, the legally relevant facts) can be expressed as legal uncertainty, vagueness or ambiguity. The problem with legal uncertainty is not a new problem, but coupled with problems with describing the facts as they relate to computers and code, the uncertainty is compounded because there is uncertainty regarding both the question of facts and the question of legally relevant facts. In terms of the primary focus of this dissertation, the meaning of "without authorization/right", the problem with describing fact and the problem with describing the law overlaps. This is so, particularly in terms of authorization with respect to outsiders, because their authorization is hinged upon the context and not a special delegation of authorization as is the case with insiders. In relation to hacking statutes, the context is computers and code.

2.1.1 Describing facts

Technology can be hard to understand. Even when it is understood, perhaps as mathematical formulas or expressions of logic, it may be hard to describe facts related to technology in useful and accurate language.

Mads Bryde Andersen wrote about problems with description in IT law in his 1988 doctorate *EDB og Ansvar* (*Computers and liability*). Although his work on this particular topic is now over 25 years old, the general observations about problems of description that relate in particular to IT law are still of interest to this day, as Andersen's thoughts are quite abstract. Professor Orin Kerr similarly addressed the problem of description as a problem with perspectives in his 2002 article *The Problem of Perspective in Internet Law*.

Andersen focuses on two problems of descriptions that relate particularly to IT law: (1) the terminology problem and (2) the generality problem.[15] The terminology problem and the generality problem in turn breed a third problem, which Andersen calls the delimitation problem.[16] The terminology problem, he explains, relates to the lack of "intersubjectivity"[17] in the IT field, and that there is a lack of clarity in the terminology.[18] The generality problem relates to the fact that the same basic components are involved in computing today, although they are smaller, faster and cheaper than in 1985. They are general purpose components that can be used to construct a variety of devices. The shared purpose and function is data processing.[19] The third problem of description, the delimitation problem, which relates to the problem that arises when trying to describe and delimit the scope of information technology.[20] There is IT in everything nowadays; our Smart TVs, mobile phones, refrigerators, and even some toilets. Delimiting IT concepts, even such a concept as "computer" is difficult, because where do you draw the line between a computer and a device that shares the same components but perhaps has another primary purpose (such as keeping your food refrigerated)? The problem is arriving at a meaningful delimitation of the field.

Even though Andersen was discussing these problems within the context of IT contract law, the problems he describes are transferrable to cybercrime law. There is arguably not much greater intersubjectivity today than there was when Andersen wrote his doctorate. The generality problem has similarly remained unaffected by the passing of time, as the same principal components, although now improved, are used in devices with different purposes and as such do not differ much from each other. Usually it is the software that reveals the purpose of a given machine, and even then, a variety of software can exist on the same machine, which in turn serves many different purposes. Furthermore, not everyone uses the same software or code for the same purpose. As Andersen predicted[21], the delimitation problem has only been exacerbated with the integration of microprocessors into most appliances as well as networking capability to the point where we have been talking for a while now about the Internet of Things (IoT). When talking about the difference

[15] See Mads Bryde Andersen: EDB og Ansvar (1988), p. 50 et seq.
[16] Mads Bryde Andersen: EDB og Ansvar (1988), p. 54
[17] Intersubjectivity arguably meaning a shared understanding between people about the meaning and use of terminology. Andersen does not provide a definition of intersubjectivity, but as he ties the concept to the "empirical aspect", which he ostensibly uses to describe decisions based on prior knowledge (seemingly experience-based). See Mads Bryde Andersen: EDB og Ansvar (1988), p. 34-35
[18] Mads Bryde Andersen: EDB og Ansvar (1988), p. 50
[19] Mads Bryde Andersen: EDB og Ansvar (1988), p. 52-53
[20] See Mads Bryde Andersen: EDB og Ansvar (1988), p. 54-55
[21] See Mads Bryde Andersen: EDB og Ansvar (1988), p. 55

between URLs and passwords as methods of access control, the two do not principally differ technically – not in a meaningful way, at least. These two concepts, URLs and passwords, and their meaning is going to be of importance in when analyzing some of the cases in the chapter on authorization with respect to outsiders.

As pointed out by Mads Bryde Anders, a legal problem that arises out of an erroneous description of the technology, may result in a relevant problem legally speaking, but in practically terms it is irrelevant. When cases involve very technical accounts that may differ depending on the whether it is the defense or the plaintiff/prosecution that is offering the account, the court (or jury) will have to choose which account it relies on. Both accounts may be objectively correct, yet one account makes the facts legally relevant, whilst the other does not. The court has to decide, perhaps without really understanding the technology, to which factual description to apply the legal rule. And this is just assuming that both technical accounts are correct. In reality, it may very well be that one or both of the accounts are based on incorrect understanding of the facts, which the court is not equipped to discover. Thus, the courts may be solving a problem that does not really exist, or at least is not relevant to the legal rule applied. Again, the framing of "secret" web addresses as being equivalent to passwords can be made to seem plausible, but in fact the function of URLs are not related to the function of passwords. In some cases it may be hard for judges to determine whether such a claim is legitimate or not, because making the right choice is largely dependent on at least some technical knowledge and experience.

This necessity of being able to understand the facts is underlined by Orin Kerr. In his 2002 article on perspectives, Orin Kerr discussed how the choice of description of the facts (as determined by the choice of perspective) could determine the outcome of cases under the CFAA and other legal rules where the facts of the case are related to computers. Kerr explains that technical facts can be described from the external and the internal perspective, which he also calls the physical world perspective and virtual perspective, respectively.[22] As Kerr explains, for example, that what the Internet is, depends on what perspective we choose. It can be perceived as a virtual world that we enter and enables us, for example, to visit the library or the supermarket, meet other people or emerge ourselves in games that again are designed to create a virtual world experience, without us ever moving in the physical world, or the Internet can be perceived as loads of interconnected

[22] Kerr's approach is based on theories of systems developed by H.L.A. Hart and others. See Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, p. 358.

hardware running programs that can exchange information through use of common agreed-upon communication protocols.[23] However, Kerr makes another excellent point: "The real produces the virtual, but the virtual need not reflect the real."[24] For that reason, choosing one or the other will result in different outcomes that are independent of each other.[25] What Kerr is driving at is that even if we experience, for example, an email client as being virtually the same as other email clients because they deliver the same results, i.e. sending mail, displaying an inbox etc., does not mean that the email clients deliver those experiences in the same way. Thus, dramatic changes in code can go unnoticed, whilst small changes in code can produce a dramatically different experience. The average user will be more focused on whether he can send and receive his email and search through his inbox than caring about how the code makes this possible for him to do and how that may differ from other email clients that may do things differently but still yield the same end-result.[26]

If the facts are misunderstood, and the law is correctly understood but applied to erroneous assumptions about the facts, the scope of the law becomes even more confusing because it departs from reality. When trying to understand something that is unfamiliar to us analogies are often helpful. However, analogies are not always accurate, and can be rooted in misunderstanding. Especially, courts ought to be careful where the analogy implies that the court must follow an existing set of rules developed in a different context. For example, the Danish legislative history indicates that gaining access to information by using the password belonging to another without permission means that the access is unauthorized. If one could convince the court that visiting a web address that has not been shared directly with that person is the same as using an ill-gotten password, then the password analogy directs the court to find that the access was unauthorized.

Many years ago I stumbled on to a website I enjoyed reading. It was a blog of sorts written by an Englishman who humorously described to his readers the cultural clashes between him and his German girlfriend. He made even the most mundane arguments humorous, such as their argument on the correct way of cutting a kiwi fruit in half. Anyway, I digress. The point of this anecdote is not the particular content of his writings nor my particular sense of humor, but what happened after I had signed up to his mailing list. After a few years of remaining on the mailing list, I received an email with a link to a page on his website that was reserved for those on the mailing list. The page, however, is entirely unprotected (it is accessible to anyone who knows the URL) apart from the fact that there is no link from the main page to this "reserved" page. In the email there was a courteous request that I not share the link with others as the page was

[23] See Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, p. 362
[24] Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, p. 362
[25] See Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, p. 362
[26] See Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, p. 362, FN 19

intended only for those on the mailing list. I have always respected the request, but not because I thought I risked being held criminally liable for sharing the link, but because – well – he asked me nicely and so far nothing has given me a particular reason to do otherwise. Now, however, after I have spent quite some time delving into what "without right"/"without authorization" means, I am not so sure what compels me more to respect the request; the faint, yet conceivable, threat of criminal prosecution based on a broad interpretation of a broad statute, or that he asked me nicely. The final point of the story is actually more of a series of questions than a statement: Should I face criminal prosecution should I ever share the link? Is a non-member who accesses the page, fully aware that it is intended only for those on the mailing list, committing the crime of access "without right" /"without authorization"? What about a non-member who manages to guess the URL of the page and becomes aware that there is no direct link to it from the main page? Or a non-member guessing the URL, or through other means stumbles onto the page (granted he would lack "intent" as to the lack of authorization, but if he can so easily find the page, why should I risk prosecution)? The link has long since been indexed by Google and appears in the search results, if you know what terms to google; would that be relevant to my defense that the page is so easily accessible to anyone, or is that entirely immaterial? Can I be (more or less unilaterally) bound to keep secret, information that is publicly accessible? Should I ever share the link or access the page after leaving the mailing list, I might be at the mercy of the writer's willingness to enforce his request and I might be at the mercy of the prosecution's interpretation of the hacking statute and later the court's interpretation. The language of the Danish and the US hacking statutes do not exempt me from prosecution at least. After all, technically, I can easily fulfil every element of the language of the typical hacking statute by leaving the mailing list and accessing the webpage afterwards. The final question: Should any of the hypotheticals above fall within the scope of a criminal hacking statute?

The anecdote above frames the general theme of the dissertation; namely, how little it takes to make a plausible-sounding case for prosecution under a typical hacking statute. There is so much discretion granted to the prosecution, the owner of the computer (or information or programs), and the courts with respect to determining what is "unauthorized". The statutory language itself does not differentiate between hacking into top secret military computer systems and my accessing the "reserved" webpage after leaving the mailing list – only the sentencing phase makes such distinctions relevant.

As for the technical details, my accessing the "reserved" webpage looks no different from any other "authorized" person's access. But is the possession of the URL the same as possessing a password? How would we differentiate between possession of this particular URL that points to an unprotected, technically publicly accessible webpage and possession of any other URL that points to publicly accessible sites? How do we even technically differentiate a URL from a password? There is no difference technically speaking. The difference lies in our perception of the two – and even then there are those that would argue that a URL can be a password even if it is completely unprotected. That is, you can make arguments for and against a URL being a password. Through

our subjective interpretation, we can let ourselves believe anything is a password as long as we just use it as if it were a password. I could claim that my phone number is the password you put into your phone that enables you to call me, and that the URL of my website is the password for accessing it. The technical aspect of URLs is rather simple; the URL points to a web resource. That is it, simplistically said. Qualifying a URL as a password is a subjective interpretation of what a URL is, based on the individual's belief as to its purpose in a specific scenario. The ability to characterize a "tool" as having a specific purpose in a specific context other than what it is usually associated with means that an interpretational problem arises before we ever get to the statutory text; e.g. the question whether a URL is the equivalent of a password (not in the legal sense, but in the factual sense). The answer to that question determines the legal outcome.

2.1.2 Describing legally relevant facts

What facts are legally relevant is determined by the legal rule. It is then quite understandable and natural that where cases involve facts that are hard to understand (and describe), and additionally involve a legal rule that is hard to understand because it uses terms that are veiled in uncertainty, it becomes exponentially harder to determine when the rule is applicable, in general, and more specifically whether the rule is applicable to the particular facts of a case. In terms of illegal access statutes, the uncertainty and lack of understanding relates equally to the facts and the legal rule; the uncertainty is compounded in cybercrime cases because the court is applying a law it may not understand to facts it may not understand. A misunderstanding on either side, the factual or the legal, affects the outcome of the case. Since the legal rule determines what facts are legally relevant, it is essential to understand the rule before applying it, just as it is important to understand the facts before applying a legal rule. Because "without right" is left to judicial discretion, the courts have some freedom to choose which facts are legally relevant facts in terms of determining whether access was with or without right. Those choices cannot be arbitrary and it has to be reasonably foreseeable what conduct triggers criminal liability.

The remainder of the dissertation involves attempting to discover an analytical framework that helps courts determining whether access was unauthorized or not. The discovery of a framework not only involves looking at "good" interpretations of unauthorized access statutes, but also cases that involved less fortunate interpretations that later turned out to produce odd or arbitrary outcomes

in other cases, or may even have been found unconstitutional – perhaps because the court started out deciding the conduct in question was wrong, and then found the arguments to support that conclusion, which is understandable at some level, since the statutory text does not give them much guidance to figure out where the line goes between legal and illegal; but such gut-feeling approaches are not desirable.

The language of the hacking statutes do not make it possible for those applying the law easily to discern between criminal conduct and innocent/desirable conduct. The statutory language is unclear as to the standard of "without right" / "without authorization". The standard can be construed to incorporate social norms, contractual obligations, agency theories, code-based access restrictions or just where the access precedes conduct that is criminal, even where the access was otherwise authorized. This is an incredibly wide spectrum of conduct, ranging from the merely annoying to seriously harmful conduct to irrelevant conduct. Much of the spectrum is defined by the owner of the computer. The owner chooses whether to incorporate code-based access restrictions, and whether to attach terms and conditions to the access of the computer. Similarly, where the otherwise authorized access precedes illegal conduct, such as illegal use of information, this opens up the scope of hacking statutes to include copyright violations, data protection violations, trade secret law violations, and so on, where violation of any of these could turn an authorized access into unauthorized access based solely on the criminality of later conduct that takes place subsequent to the access, effectively letting the legally relevant facts be determined by other statutes, so that violation of those statutes automatically carry with them a violation of hacking statutes. The question is whether all of these are relevant facts that can trigger liability under an unauthorized access statute.

2.2 A comparative perspective

At first it might not seem relevant to seek a comparative perspective in US law whilst also operating with Danish and international law, mainly because the legal systems differ in many respects. In most areas of law, it might be more relevant to look closer to home, such as neighboring countries with familiar legal systems, to seek comparative inspiration as to the legal status and legislative approaches to solving complex problems. This may be true for most areas of law. However, as previously explained, US law is interesting 1) because there is an abundance of case law regarding

the federal hacking statute in all sorts of factual contexts, 2) because the courts extensively explain the reasoning for their decision to apply or reject to apply the statute, and 3) because the statute they apply is very similar to the Danish provision, and also 4), like the Danish hacking provision, serves to implement the Convention on Cybercrime.

3 SOURCES OF LAW AND OTHER AUTHORITES

The purpose of this chapter is to describe the sources of law that are relevant to this dissertation, and delineate the extent of their authority. The following chapter on interpretation and construction will sketch the rules of interpretation and construction that relate to the application of these sources of law in the individual legal systems. Descriptions will be relatively brief, because the more complex question is how to put the legal sources into action rather than merely stating their existence and their role.

The purpose of touching upon sources of law in the various legal systems is two-pronged: First, the various legal systems' approach to cybercrime legislation has directly and/or indirectly influenced each other. As will be explained later, the 1985 Danish hacking statute seems to have been at least partially inspired by US experiences with computer crime (which itself ostensibly seemed to be, at least partially, a reaction to the 1983 movie WarGames[27]). Later, in the late 90s and early 00s, due to its vaster experience with computer crime, the US appears to significantly influence the drafting of the Convention on Cybercrime.[28] A couple of years later, the Convention's substantive articles are essentially imported into an EU framework decision, the content of which still lives on in a directive and thus creating a legally binding EU measure that must be implemented in member states. Second, because of this apparent relationship between the various hacking legislations (and even if there is no clear causal link between the Convention's scope and US influence, the fact remains that the language of hacking provisions are very similar because the Convention was meant to harmonize national criminal law) the legislations suffer from the same problems related to their interpretation and construction, and thus, ultimately, their potential practical application. The potential scope of application is in turn affected by other laws that directly or indirectly affect how a source of law must be interpreted. Rules of interpretation and construction may act as some sort of referees by determining what influence one source of law has on the application of the other.

The first section of this chapter concerns international law. The source of harmonization, so to speak, is the Convention on Cybercrime. Denmark and other EU member states are also bound by

[27] See reference to WarGames in the House Report on (the then proposal of) the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, H.R. Rep. 98-894 at *10-11

[28] See more in later chapters on e.g. the Convention on Cybercrime and the US law (the CFAA). See also Michael A. Vatis: The Council of Europe Convention on Cybercrime (2010), Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Available at http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf.

the European Convention on Human Rights (ECHR) (as well as domestic constitutional rights which fall outside the scope of this dissertation) and implementations (if required by domestic law) and subsequent applications of the criminal provisions must be in conformity with the ECHR.

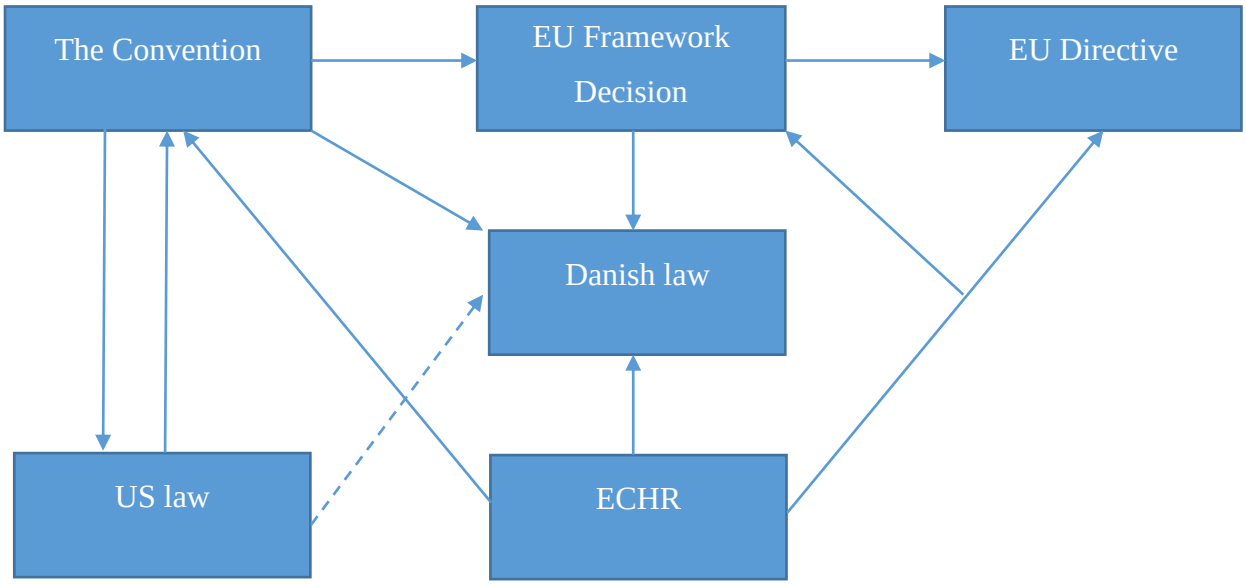
Whereas the EU cybercrime legislation and the Danish legislation are subject to ECHR requirements, the US legislation is subject to domestic constitutional requirements. These non-criminal law sources of law affect how and if a criminal law provision can be applied.

Since EU law affects Danish law to an extent in the cybercrime area, the second section describes the source of law within the EU system and how these sources of law affect application of implementations of EU law in the domestic courts.

The third section, outlines the sources of law in the US legal system, since this dissertation seeks inspiration in US case law in terms of how hacking statutes have been applied; more specifically, how key elements common to most, if not all, hacking statutes have been construed by US courts. The section furthermore describes how international sources of law are treated within the US legal system rather than how they are expected to be treated seen from an international law point of view. That is, international law does not have effect in national law unless the domestic legal system enables it to have effect.

The fourth section addresses sources of law in the Danish legal system and how Danish courts perceive and may apply e.g. conventions, EU law, etc. That is, whereas the section of international law describes how, from an international law point of view "looking down", international sources of law ought to be applied, the section on Danish law – as well as the section on US law – describes how these international sources of law are treated seen from inside the domestic legal system "looking up".

The drawing below illustrates the connections described above.



3.1 International law

International law concerns itself with the legal relationship between sovereign states.[29] Questions regarding the deeper meaning of the existence or non-existence of international law, whether international law is really *law*[30], what defines a sovereign state, and so on, fall outside the scope of this dissertation. For the purpose of this dissertation, the existence of international law is unabashedly presumed.

Not all problems are capable of being solved within the confines of national law. Especially so, when the problem involves interests of other states. This dissertation will focus solely on treaties, conventions and the likes, and not jus cogens (international customary law).[31]

It is clear that in absence of a supreme power that enforces international law when states misbehave, international law is only binding insofar as national law recognizes it as binding. The Vienna

[29] Ole Spiermann: Moderne folkeret (2006), p. 1
[30] One of the more typical questions being: Is something really binding and therefore law if it cannot be enforced?
[31] For the purposes of this dissertation, it is primarily international law in the form of treaties that is of interest rather than international customary law. International customary law will thus not be the subject of any particular discussion as such.

convention on the law of treaties[32] expresses a rule generally accepted as a general principle of international law[33]:

> Article 26. "PACTA SUNT SERVANDA"
>
> Every treaty in force is binding upon the parties to it and must be performed by them in good faith.

The International Court of Justice (ICJ) has noted that pacta sunt servanda and fulfilling obligations are separate issues.[34] According to the ICJ, a treaty may be binding even though the duties under the treaty are not carried out. The ICJ further noted, that the purpose of the treaty and the intentions of the parties to the treaty out-weight a literal application. This, the ICJ, couples with the principle of good faith application of the treaty in order for the treaty to fulfil its purpose.[35] For this reason, chapter 6 on sources of law also addresses when international law, more specifically treaties in the context of this dissertation, is binding upon the US and Denmark also as seen from national law, and what role the binding and non-binding texts might play in national law and courts when applying either the treaty itself, or provisions in national law that serve to fulfil treaty obligations.

3.1.1 The Council of Europe Convention on Cybercrime

The Council of Europe's (CoE) Convention on Cybercrime and its accompanying explanatory report was adopted on 8 November 2001 by the CoE's Committee of Ministers, and was opened for signature in Budapest on 23 November 2001.[36] The conditions for the Convention entering into force were the ratifications by five signatories of which at least three were member states of the Council of Europe.[37] The Convention entered into force on 1 July 2004. Fifty-four states are signatories to date, and 47 out of those 54 states have ratified/acceded to the Convention. Canada is

---

[32] Note that although the United States has not ratified the Vienna Convention, the U.S. generally recognizes it as customary international law. See Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 2, FN 7 (citing as example Fujitsu Ltd. v. Federal Exp. Corp., 247 F.3d 423 (2nd Cir. 2001))

[33] Or alternatively, an international custom. See Ole Spiermann: Moderne folkeret, p. 61

[34] Ole Spiermann: Moderne folkeret (2006), p. 61, citing Gabcíkovo-Nagymaros Project, ICJ Reports [1997] 7, para. 142

[35] Ole Spiermann: Moderne folkeret (2006), p. 61-62, citing Gabcíkovo-Nagymaros Project, ICJ Reports [1997] 7, para 142

[36] Explanatory report, para. I

[37] The CoE's website listing signatories to the Convention at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG. Last visited on 4 August 2015.

the latest state to ratify the Convention, which it did on 8 July 2015.[38] Only member states of CoE and those non-member states that participated in the negotiation/drafting process of the Convention were eligible as signatories until the Convention entered into force.[39] Other non-member states may be invited to accede to the Convention after the Convention entered into force.[40]

The Convention has three explicitly stated aims. First, harmonization of substantive national criminal law provisions in the area of cybercrime. Second, providing national procedural law powers to investigate cybercrime. Third, establishing a regime for international cooperation.[41] The Convention addresses an international problem that concerns the interests of every nation state and a problem that cannot be solved solely within any one nation state.

An explanatory report was negotiated and drafted in the Committee of Experts alongside the Convention, was adopted at the same time as the Convention. It does not provide an authoritative interpretation of the Convention's provisions, but may be useful when applying the provisions.[42] Because the provisions in the Convention use terms that are, on their face, devoid of clear meaning or ambiguous, the explanatory report gives a more detailed account of the intended application of the provisions and how individual concepts were understood.

Recalling the Vienna Convention's article 31, the explanatory report is such a text, which was adopted by the Committee of Ministers of the Council of Europe along with the Convention on Cybercrime, and may serve as an aid in interpreting the Convention, regardless of whether it is binding or not. In other words, it is capable of having persuasive authority, but is not binding.

To summarize briefly, the Convention on Cybercrime obligates the parties to criminalize certain cybercrimes within their national legal system. Hence, the Convention serves to harmonize rules that regulate the relationship between a sovereign state and its citizens and requires the introduction or expansion of the powers the state that may wield against the citizens at the national level; it restricts freedom and expands powers to investigate violations of the required restrictions (criminalized acts).

---

[38] Chart of signatures and ratifications, available at CoE's website (http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG). Last visited on 4 August 2015.
[39] Convention on Cybercrime, article 36(1) (the non-member states were the United States, Canada, South Africa and Japan)
[40] Convention on Cybercrime, article 37(1)
[41] Explanatory Report, para. 16
[42] Explanatory Report, para. II

3.1.2 European Convention on Human Rights (ECHR)

Even though article 15 of the Convention on Cybercrime only applies to the procedural powers, it does not follow that the lack of application to the substantive part means that any implementation and application of the substantive part is free from scrutiny under human right treaties and/or rights provided for under domestic law. One of the most relevant human rights treaties in the context of this dissertation is the European Convention on Human Rights, which applies to Denmark and other European Union member states, and thus affects the application of the implementations of the Convention on Cybercrime and EU cybercrime legislation.

Also a product of the Council of Europe, the ECHR[43] entered into force on 3 September 1953.

The ECHR obligates its signatories to "secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention."[44] Among the rights in Section I of the Convention, and of great relevance to the topic of this dissertation, is article 7 ECHR, which prohibits punishment without law (*nullum crimen, nulla poena sine lege*).

Article 19 ECHR establishes the European Court of Human Rights (ECtHR) in Strasbourg. The Court's role is to "[t]o ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols thereto […]"[45]. The decisions rendered by the ECtHR are binding upon the parties to the case, and the judgments are final.[46] Furthermore, the ECtHR may give advisory opinions as to the interpretation of the Convention and its protocols.[47]

As opposed to the Convention on Cybercrime, the ECHR is enforced by a court capable of rendering final and binding decisions, as well as the Court being able to secure a certain uniformity in the application of the ECHR. This lack of control mechanism in regards to the interpretation and application of the Convention on Cybercrime results in significantly different approaches to the subject-matter, as will be elaborated upon in later chapters in the dissertation.

The role of and application of the ECHR within the EU and in Denmark is further discussed below and in the chapter on interpretation and construction.

---

[43] Also known as Convention for the Protection of Human Rights and Fundamental Freedoms, ETS no. 005
[44] ECHR article 1
[45] ECHR article 19
[46] ECHR, article 46
[47] ECHR, article 47

3.1.2.1 The relationship between ECHR and the Convention on Cybercrime

According to the Convention on Cybercrime's article 15, parties to the Convention must "ensure that the establishment, implementation and application of the powers and procedures" provided for in the section on procedural rules (rules expanding police investigative powers) "are subject to conditions and safeguards provided for" under the party's domestic law as well as those conditions and safeguards that flow from international human rights obligations, such as the ECHR. Article 15 of the Convention on Cybercrime thus only applies to the expanded procedural rules. Only in the Convention's preamble is there a more general statement reminding of the need to balance the interests of law enforcement and respect for human rights, such as freedom of expression, including seeking, receiving and imparting information.[48] The preamble specifically refers to the rights in ECHR and UNCPR[49].

3.2 EU Law

The European Union has also passed cybercrime legislation. European Union law is supranational law and is the product of the legislative bodies of the European Union as it is interpreted by the Court of Justice of the European Union. Member states have ceded sovereignty in certain areas, which then are regulated either exclusively by the EU or by the EU and the member states concurrently.[50] In any remaining areas, the member states, as sovereign states, can govern as they see fit, although legislation or practices that interfere with the fundamental freedoms are subject to the supremacy of EU law and other general principles in EU law.

As opposed to US law, European Union citizens cannot file suit directly with the Court of Justice, and therefore do not have standing in that sense. Rather it is the national court that petitions the CJEU, requesting it to rule on a preliminary question regarding application of EU law in a case before it.

[48] Council of Europe's Convention on Cybercrime, preamble para. 10 (not enumerated in the Convention's text)
[49] 1966 United Nations International Covenant on Civil and Political Rights
[50] See Treaty on the European Union, article 5, and enumeration of competences, exclusive, concurrent or supplementing in the Treaty on the Functioning of the European Union, articles 2 through 6.

The Court of Justice's jurisdiction is to interpret EU law and promote uniform application of EU law[51], but it does not interpret member state laws as such. To understand EU law and its interaction with national legal systems a little history does not hurt, especially with a view to understanding why Denmark's status differs from the vast majority of other member states in the cybercrime area.

3.2.1 Formation of the Union

In the wake of two world wars, a war weary Europe sought to prevent further armed conflicts in the region. In 1950, Robert Schuman, the French minister of foreign affairs, suggested that European states enter into a collaboration, which would place the coal and steel industry, both integral to war-related production, under a single organization. What came to be known as the Schuman plan, envisaged independent institutions competent of issuing decisions binding on all member states, which in turn presupposed member states ceding sovereign powers to the institutions. The plan envisaged a collaboration that would grow more tight-knit over time and that could eventually pave the way to the formation of a European federation.[52]

In 1951, France, Germany, Italy, Belgium, the Netherlands and Luxembourg ratified the Treaty establishing the European Coal and Steel Community (ECSC; also known as the Treaty of Paris). It was the first supranational collaboration of its kind. The treaty entered into force in July 1952, and would expire 50 years later in July 2002.[53]

In 1957, two additional treaties were signed in Rome; Euratom and the Treaty establishing the European Economic Community (EEC), both of which entered into force on 1 January 1958. The EEC aimed to create a common market and to integrate economic policies in member states, affecting a much larger portion of the industry than just steel and coal.[54] The EU can only legislate within the framework of the powers conferred upon it. These areas are enumerated in the treaties.

Denmark, along with the United Kingdom and Ireland, joined the community in 1973.

In 1993, the Treaty of Maastricht established the Treaty on the European Union, adding the fourth treaty to the collaboration. With the Treaty of Maastricht came the three pillars. The first pillar consisted of the original economic collaboration. The second pillar consisted of common foreign

[51] See generally article 19 TEU
[52] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 25 et seq.
[53] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 25 et seq.
[54] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 26

and security policy. The third pillar concerned justice and home affairs (later narrowed to police and judicial cooperation in criminal matters). The first pillar operated at the supranational level, whilst the second and third pillars operated at an intergovernmental level.

In Denmark, the public voted against the Treaty of Maastricht. This led to the adoption of the Edinburgh decision in which Denmark made reservations limiting the obligation to participate fully in the collaboration. These reservations were in regard to the collaboration under the second and third pillars, the union citizenship and the participation in the euro cooperation.[55] However, the reservation pertaining to the union citizenship is considered largely symbolic having no real legal effects.[56] Any legislation adopted under the second and third pillar would not bind Denmark. This did not preclude Denmark from occasionally opting in on second and third pillar legislation in certain cases.

Although the pillar system was abolished in 2009 when the TFEU absorbed the third pillar into what is now the European Union, some of the legislative acts adopted under the third pillar remain. The aim is to convert these remaining legislative instruments into regulations and directives. The areas covered by the third pillar have therefore moved from the intergovernmental level to the supranational. This introduces an interesting, and rather convoluted, problem regarding the framework decision on attacks against information systems and its status post-Lisbon with respect to Denmark. This will be discussed further below.

3.2.2 Sources of law in EU law

3.2.2.1 Primary law

The treaties and the Charter on Fundamental Rights of the European Union (the Charter) are primary legislation. The secondary legislation has its legal basis in the treaty and can only be adopted within the scope of the treaty, as well as it must comply with the Charter and the general principles of EU law. For example, article 114 TFEU, which in some aspects resembles the "commerce clause" in the US Constitution, serves as a legal basis for secondary legislation regulating aspects of the internal market. When regulating the internal market, the secondary legislation adopted under article 114 TFEU, may include criminal sanctions, cf. C-176/03

[55] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten, p. 31
[56] Ulla Neergaard and Ruth Nielsen: EU ret (2010), p. 675

Commission v. Council. After the third pillar was abolished, the legal basis for secondary legislation relating to harmonizing member state criminal laws may be found in article 83 TFEU[57] in the Chapter on an area of freedom, security and justice. Article 83 TFEU allows the Council and the EU-Parliament, following the ordinary legislative procedure, to adopt directives on criminal law setting out the minimum rules for which acts to criminalize as well as the punishment associated with committing the acts.

The EU Charter on fundamental rights started out as soft law when it was adopted at a meeting in European Council December 2000. As of the entry into force of the Lisbon treaty, the Charter now has the same status as the treaties.[58] The Charter provides for numerous fundamental rights, many of which overlap with rights enshrined in the ECHR. The significance of the Charter rights of relevance to this dissertation, namely article 49 of the Charter, is explained briefly below in the section on the relationship between the EU, the Charter and the ECHR.

3.2.2.2 Secondary law

Regulations, directives, and decisions are secondary law adopted in accordance with the appropriate legal bases provided by the TFEU. Regulations are directly applicable and binding in all aspects[59], and generally may not be transposed into national law[60]. Regulations directly obligate both the member state and private actors.[61]

Directives are binding in terms of their aim, but discretion is left to the member states on how to transpose the directive into national law, cf. article 288 TFEU. Directives are sometimes capable of having direct effect. The possibility of direct effect of directives does not follow directly from the treaties, but from the CJEU's case law. This led to the member states' explicit statement under the old article 34 (2)(b) TEU that framework decisions could not have direct effect. From the time a directive has been adopted and until the deadline for transposing it into national law, member states

[57] Prior to the Lisbon treaty, legislative action in the area of criminal law had its legal basis in article 34 EU. Article 34 EU required unanimous agreement in the Council. Today a member state has a veto right as to proposed criminal legislation under article 83 TFEU.
[58] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 202
[59] Article 288 TFEU
[60] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 223
[61] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 223

have a duty not to act in ways that would impede the goals of the directive; a so-called *stand-still* obligation[62].[63]

Framework decisions were the legislative instrument used in the third pillar, cf. pre-Lisbon article 34 EU, and operate at an intergovernmental level, although institutions other than the Council play a limited role,[64] whereas directives operate at the supranational level. Like directives, they are binding as to their purpose and object, but member states have discretion as to the form and methods of implementation in national law.[65] As opposed to directives, framework decisions are incapable of having direct effect, cf. article 34 (2)(b) EU (pre-Lisbon). However, as will be explained in the chapter on interpretation and construction, framework decisions do have "indirect effect".

3.2.3 Case law

The case law of the Court of Justice of the European Union plays a prominent role when one seeks to determine what the law is in any given area of EU law; not entirely unlike the common law tradition (studying EU law requires significant case law studies). Authoritative interpretation of EU law is the prerogative of the CJEU, which ensures uniform interpretation and application of EU law in the member states. Member state national courts can in turn, and in some cases are obligated to, request preliminary rulings from the CJEU on the interpretation of EU law. Only the CJEU has the competence to annul EU legislation. National courts cannot decide upon EU law validity.

Advocate Generals assist the Court by supplying a thorough analysis of facts and law relevant to the case, resulting in a recommendation to the Court.[66] Opinions of Advocate General are not binding upon the Court and the Court does not always follow them.[67] Their usefulness lies in that the opinions can give an insight into the reasoning behind the Court's decision, when it does follow the recommendations of the Advocate General, and generally cast a light on the issues at hand.[68] In

[62] Similar principles follow from international law. See the Vienna Convention's article 18.
[63] Ulla Neergaard and Ruth Nielsen: EU-ret, p. 223
[64] Josephine Steiner and Lorna Woods: EU Law (2009), p. 73
[65] Josephine Steiner and Lorna Woods: EU Law (2009), p. 74
[66] Josephine Steiner and Lorna Woods: EU Law (2009), p. 45
[67] Josephine Steiner and Lorna Woods: EU Law (2009), p. 45 and Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 158
[68] Josephine Steiner and Lorna Woods: EU Law (2009), p. 45 and Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 158

addition, the opinions often contain discussions that are more theoretical and as well as containing references to literature, which can give a valuable insight into the particular area of law.[69]

3.2.4 The relationship between the EU, the EU Charter and the ECHR

Even before the EU acquired the explicit competence to accede to the ECHR, the CJEU had acknowledged the ECHR as an influence on EU law. The CJEU has referenced the ECHR in numerous cases, and in 2010, the ECtHR also revised their interpretation of an ECHR right in light of the EU Charter on fundamental rights.[70]

To avoid conflict between the ECtHR and the CJEU, it is stated in the Charter's article 52 (3), that insofar as the Charter contains rights corresponding to those rights contained in the ECHR, the rights in the Charter have the same meaning and scope as those of the ECHR. However, that does not preclude the Charter from providing more expansive protection than the ECHR.

The EU has not as of yet acceded to the ECHR with the CJEU rejecting the draft agreement on EU accession as being incompatible with EU law in December 2014.[71]

[69] Ulla Neergaard and Ruth Nielsen: EU-retten (2010), p. 158
[70] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), s. 199-200
[71] Opinion 2/13 of the Court of 18 December 2014. Available at http://curia.europa.eu/juris/document/document.jsf?docid=160882&doclang=EN. Last visited on 5 August 2015.

3.3 US Law

3.3.1 The US legal system and sources of law

The US legal system has evolved in its own distinct manner since the US severed its connection with the Crown of England. Although English decisions were cited in the earlier days due to various factors, this is rarely the case today.[72] Nevertheless, the US legal system was, in its infancy, heavily influenced by English law and its origin is found in English law, which is not surprising given the origins of many of those who immigrated to the New World. Remnants of influence from other legal systems can also be found in many states. For example, Louisiana, the only US "civil law" state, was heavily influenced by French law. Influence can also be seen in states formerly occupied by Spain and Mexico. The foremost ideas inherited from English law include the concept of the supremacy of law, tradition of precedent and a trial as a contentious proceeding.[73]

The US Constitution grants powers to the federal government only in limited areas, such as taxation and the authority to wage war. In some areas, federal legislative authority is exclusive, while in others the authority to legislate is concurrent. In any remaining cases, where federal authority is not exclusive or concurrent, the individual states are still sovereign, and the validity of state legislation is subject only to the US Constitution.[74] The validity of federal legislation is equally subject to judicial review in federal courts.[75] [76]

In the hierarchy of sources of law, the Constitution is the highest ranked in that it is the "supreme law of the land". Federal statutes and treaties entered into by the United States are of equal authority, subject only to the Constitution. Should federal statutes and treaties conflict, the most recent prevails.[77]

In areas of concurrent powers, both state and federal courts have jurisdiction and the plaintiff can file suit in either jurisdiction. Therefore, federal courts often have to apply state laws, and vice versa, as the parties may rely on rights on the state and federal level respectively, creating a complex conflict for the federal or state court to resolve.[78]

---

[72] See more E. Allan Farnsworth: An Introduction to the Legal System of the United States, chapter 1
[73] E. Allan Farnsworth: An Introduction to the Legal System of the United States, p. 15
[74] Fletcher v. Peck (1810), US Supreme Court
[75] Marbury v. Marshall (1803), US Supreme Court
[76] E. Allan Farnsworth: An Introduction to the Legal System of the United States, chapter 1
[77] E. Allan Farnsworth: An Introduction to the Legal System of the United States, chapter 6
[78] E. Allan Farnsworth: An Introduction to the Legal System of the United States, chapters 4, 6 and 7

The tradition of precedent, or stare decisis, is one of the ideas inherited from the English legal system. When the facts of an earlier case are similar to the facts of a later case, the rule of law established in the earlier case applies to the later case. This is subject to some important limitations, the most important of which is the division of the cases into binding and persuasive authorities. A prior decision in a case with similar facts, is only binding upon the court deciding the later case, if the prior decision was made by a higher court in the same jurisdiction or if the prior decision was made by the same court. An additional, and equally important limitation, is the distinction between "holding" and "obiter dictum". The holding represents the rule of law, which was necessary to reach the decision, whereas dictum is something the judges have said in passing, but is not necessary to reach a decision in the case at hand. Dictum is persuasive authority, on par with secondary authorities such as law review articles, dictionaries, encyclopedias and so on.[79] These principles are important with respect to the significant number of US federal cases analyzed in this dissertation.

In US law, criminal law exists at both the state and federal level. The criminal law is largely statutory. Federal criminal law is reserved for the regulation of investigation and prosecution of specified crimes with an interstate dimension. Common law crimes[80] have been abolished at the federal level, as such ex post facto criminalization was deemed unconstitutional by the Supreme Court in *US v. Hudson and Goodwin* in 1812. Some states still recognize common law crimes, but in most states, criminal law is statutory, like federal criminal law.

Case law cannot alter statutes. Courts can decide upon the validity of the legislation. "Command of the legislature is supreme except in point of validity of the statute itself."[81]

The role of legislative history and purpose in US law is not without its complexities, and opinions are divided on the use of legislative history in statutory construction.[82] In any case, legislative history is not called upon unless the statute's language is ambiguous.[83] The legislative history of

[79] E. Allan Farnsworth: An Introduction to the Legal System of the United States, chapter 5
[80] Common law crimes are crimes mala in se, or crimes thought to be inherently wrong or evil, such as murder. The creation of common law crimes was gradually abandoned in the US, although not for reasons of retroactivity. See more, Oxford Handbook of Comparative Law: Markus Dirk Dubber: Comparative Criminal Law
[81] E. Allan Farnsworth: Introduction to the Legal System of the United States (2010), chapter 7
[82] Wayne R. LaFave: Criminal Law (2010), p. 99
[83] E. Allan Farnsworth: Introduction to the Legal System of the United States (2010), chapter 7. See also Wayne R. LaFave: Criminal Law (2010), p. 97 and FN 54 on the same page.

federal statutes is very well documented compared to state legislation.[84] Committee reports form the House and the Senate generally paint a picture of the existing legislation and the intended scope of proposed legislation, and it is generally accepted that Congress adopts the committee's intent in terms of the details.[85] However, the role of legislative history in the construction of criminal statutes is perhaps somewhat more limited due to fair notice reasons, and the rule of strict construction of criminal statutes.[86]

3.3.2 The Cybercrime Convention and US Law

The United States was granted observer status with the Council of Europe on 7 December 1995.[87] As a non-member country, the US is offered the opportunity to co-operate with the Council. This entails e.g. "accepting guiding principles of democracy, the rule of law, human rights and fundamental freedoms and to send observers to [the Council's] expert committees and conferences of specialised ministers."[88] In Budapest, on 23 November 2001, the United States signed the Council of Europe's Convention on Cybercrime. The US was the first non-member state to ratify the Convention, but in recent years, five additional non-member states have joined its ranks.[89] The United States Senate voted on 3 August 2006[90] to ratify the Council of Europe's Convention on Cybercrime (attaching six reservations and five declarations, one of which declares that existing US law fulfils the obligations related to the convention's substantive provisions), and instrument of ratification was deposited on 29 September 2006. The Convention entered into force in the US on 1 January 2007.[91]

However, the Convention's substantive provisions are not self-executing and from the wording of the provisions, explicitly require implementation into domestic law to have any legal effect. The

---

[84] E. Allan Farnsworth: Introduction to the Legal System of the United States (2010), chapter 7. See also Wayne R. LaFave: Criminal Law (2010), p. 97
[85] Wayne R. LaFave: Criminal Law (2010), p. 97
[86] Wayne R. LaFave: Criminal Law (2010), p. 99. Note, however, the inconsistent application of the rule of lenity discussed later in the dissertation.
[87] Resolution (95) 37 on observer status for the United States of America with the Council of Europe. http://www.coe.int/t/der/docs/CMRes9537USA_en.pdf. See also http://www.coe.int/en/web/portal/united-states.
[88] What is observer status? The Council of Europe's website. http://www.coe.int/en/web/portal/what-is-observer-status-
[89] Australia, Japan, Dominican Republic, Mauritius and the Philippines.
[90] https://www.congress.gov/congressional-record/2006/8/3/senate-section/article/s8901-2
[91] Council of Europe's website. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=14&DF=&CL=ENG

Senate Committee on Foreign Affairs, in its advice, opined that no implementation was needed as federal law already covered the acts in the Convention's Chapter II.[92] It is important to note that because the Convention on Cybercrime is clearly non-self-executing concerning the substantive provisions it is not binding federal law, despite its ratification and despite the language of the Supremacy clause.[93] There are however provisions in the Convention that are ostensibly self-executive, in that they can serve as a legal basis for extradition.[94] At least one thing is clear, when interpreting a treaty, the court looks to the text of the treaty. To aid in interpreting that text, the court can furthermore look to the negotiating and drafting history of the treaty as well as any post-ratification understanding of the signatories to the treaty.[95]

The remaining question is, whether a non-self-executing treaty that does not require implementation into domestic law, because domestic law is considered as already fulfilling the treaty obligations, has any bearing on the interpretation of the domestic provisions in domestic courts. More specifically, can a non-self-executing treaty affect the scope of the domestic law that the Senate claimed fulfilled the obligations under the treaty. The chapter on interpretation and construction touches upon this issue.

It is not uncommon for the US to add so-called RUDs (reservations, understandings and declarations) to treaties, and US courts will interpret the US's international obligations in the light of those RUDs[96].[97] As mentioned previously, one of the RUDs associated with the Senate's advice and consent, was that existing US law complies with the obligations under the Convention on Cybercrime's substantive provisions.

The Department of Justice (DoJ) has stated that the US had "a real voice in the drafting process" of the Convention.[98] Furthermore, the DoJ stated that no legislative implementation was needed due to the US delegation's hard work in balancing "attentiveness to the suggestions of other countries with

---

[92] Senate Executive Report 109-6, 11 November 2005, accompanying Treaty doc. 108-11 (Convention on Cybercrime)
[93] This is explained further in the chapter on interpretation and construction in US law.
[94] See Council of Europe's Convention on Cybercrime, ETS no. 185, article 24
[95] *Medellín v. Texas*, 128 S. Ct. 1346, 1357 (2008) ("Because a treaty ratified by the United States is "an agreement among sovereign powers," we have also considered as "aids to its interpretation" the negotiation and drafting history of the treaty as well as "the postratification understanding" of signatory nations.")
[96] Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 4
[97] Even though the RUDs may seek to define or limit the obligations of the United States under the treaty, the RUDs should presumably be seen also in light of the Vienna Convention's article 18, which obliges states to refrain from taking actions that undermine the purpose and object of the treaty. As mentioned previously, the US has not ratified the Vienna Convention, but recognizes it as customary international law.
[98] Cache of the Department of Justice website (now defunct, but a cached version was accessed through the Wayback Machine) at https://web.archive.org/web/20111015051110/http://www.cybercrime.gov/COEFAQs.htm#QA2

respect for the strengths of current U.S. law. As a result, the central provisions of the Convention are consistent with the existing framework of U.S. law and procedure."[99] Furthermore, the DoJ notes that "the United States sought and obtained several important revisions to the Convention's text and Explanatory Report."[100] Addressing the generality of the substantive provisions in articles 2-5, the DoJ stated that the "ER [Explanatory Report] describes in more detail the kind of conduct to be criminalized under the Convention to ensure that Parties implement the Convention consistently."[101]

Furthermore, the DoJ lists a series of paragraphs from the explanatory report in response to a question regarding concerns about criminalization of legitimate activities: "While ER para. 38 explains that national law will determine precisely how to exempt legitimate activity, para. 41 makes clear that offenses must be drafted with sufficient clarity and specificity to provide foreseeability as to the conduct that will be criminalized. Moreover, ER paras. 38, 46-48, 58, 62, 68-69, 77 and 89-90 specifically provide that legitimate and common operating or commercial practices should not be criminalized."[102] Paragraph 47 of the explanatory report, which is listed by the DoJ, contains a very specific, clearly worded exception from criminalization that the US has not observed in practice; an oddity considering the DoJ explicitly cites the need for consistent implementation in party states in its reference to the explanatory report when responding to questions that relate to concerns over too broad criminalization. This paragraph is discussed later in the dissertation in connection with the chapter on outsiders and authorization.

[99] Department of Justice website (now defunct, but a cached version was accessed through the Wayback Machine) at https://web.archive.org/web/20111015051110/http://www.cybercrime.gov/COEFAQs.htm#QA2
[100] Department of Justice website (now defunct, but a cached version was accessed through the Wayback Machine) at https://web.archive.org/web/20111015051110/http://www.cybercrime.gov/COEFAQs.htm#QA2
[101] Department of Justice website (now defunct, but a cached version was accessed through the Wayback Machine) at https://web.archive.org/web/20111015051110/http://www.cybercrime.gov/COEFAQs.htm#QA2
[102] Department of Justice website (now defunct, but a cached version was accessed through the Wayback Machine) at https://web.archive.org/web/20111015051110/http://www.cybercrime.gov/COEFAQs.htm#QA2

3.4 Danish Law

3.4.1 The Danish legal system and sources of law

The Danish legal system is a Scandinavian civil law system[103], as well as being a member state in the European Union. It differs from traditional continental civil law systems in that the civil law aspect, such as that regarding law of obligations, is not codified, but rests on judge-made law.[104] However, the criminal law is entirely codified, and "common law"-esque crimes (judge-made crimes) were abandoned almost 150 years ago.[105] The courts are not formally bound by prior decisions (be it their own or those from higher courts), but in practice prior decisions from higher courts influence lower court decisions since the lower courts otherwise risk seeing their decisions reversed on appeal.[106] The Supreme Court has also been known to cite its own earlier cases when rendering decisions[107], something which is not characteristic of civil law system.[108] However, unlike courts in common law countries, Danish courts rarely attach any detailed arguments for the holding or obiter dictum[109] to their decisions, which often leaves the court's reasoning a bit on the obscure side.

The Constitution (Grundloven) is the highest ranked in the hierarchy of sources of law.[110] The Danish Supreme Court has indicated that in case of a conflict between the Constitution and EU law, the Constitution is controlling; despite the principle of supremacy developed in EU law.[111] (Note that the CJEU may take a different position on this question.) In terms of the topic of this dissertation, the Constitution plays no great role, and will only be subject to limited discussion.

---

[103] See Joseph Lookofsky: Precedent and the Law in Denmark (2006), Danish National Report, XVIIth Conference of the International Academy of Comparative Law ("Although Scandinavian legal traditions are in many respects closer to those of continental Europe than to Anglo-American law, the "Scandinavian family" is surely best placed in its own category (conceptually distinct from both Civil and Common law). Moreover, since the judgments (opinions) rendered by Danish courts differ significantly from those rendered in other Scandinavian jurisdictions (i.e., Norway and Sweden), the Danish concept of precedent is probably best described as occupying its own unique position on the "precedential" scale." (citations omitted)

[104] Joseph Lookofsky: Precedent and the Law in Denmark (2006), Danish National Report, XVIIth Conference of the International Academy of Comparative Law

[105] See e.g. Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 89

[106] Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 31

[107] The most recent example being Case 146/2014 of 28 January 2015 where the Supreme Court cited and followed its own decision in UfR 1982.126.

[108] See more on precedents in Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 151 et seq.

[109] Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 148

[110] Peter Germer: Statsforfatningsret (2007), p. 21

[111] See U 2003.1328H, p. 1331 (finding that there was no reason to assume that national constitutional law had been violated, indicating that had there been a conflict, national constitutional law would be controlling). See also Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 172

Most rules and rights of significance with respect to addressing vagueness in criminal law are found in the Criminal Code itself and in the ECHR (as well as EU law where application of EU law principles are triggered). The Danish Constitution contains no rules that address vagueness in criminal law. Furthermore, the Supreme Court does not interpret the Constitution expansively with regard to constitutional rights, more or less implicitly paying significant deference to the legislative power the Constitution has vested in the Parliament.[112] Although possessing the power to rule on the validity of legislation, the courts almost never exercise this power[113]; even if they were inclined to exercise this power more liberally, there is no constitutional basis for challenging the validity of legislation on account of vagueness, since the Constitution does not provide any such guarantees. This will be addressed further in the chapter on nullum crimen sine lege.

The main statutory criminal law legislation is the Criminal Code of 1930.[114] The Criminal Code contains the most serious crimes, whilst special criminal law consists of provisions providing for criminal liability and punishment in various statutes, for example the Data Protection Act. Executive orders (orders issued by ministers pursuant to a statutory delegation of power to regulate; typically in more detail) may also contain provisions providing for criminal liability and punishment insofar as the enabling statute allows for it.[115] The Criminal Code expresses the principle of legality in § 1[116], which requires there to be a statutory legal basis for criminal liability and punishment. However, § 1 also allows for a "complete statutory analogy"[117]; meaning that a criminal conviction can be based on an analogy, if the conduct in question is completely analogous to the conduct criminalized by statute. This will also be subject to further discussion in the chapter on nullum crimen sine lege. The Criminal Code § 2 states that the principle of legality also applies to criminal provisions in special legislation.[118]

Legislative history is not a source of law.[119] However, there is a rich tradition in Denmark of using legislative history as an interpretive aid (subjective interpretation[120]). Subjective interpretation is

[112] Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 29
[113] Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 29
[114] Last amended on 9 July 2015.
[115] Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 31
[116] It has done so since 1866. See Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 30
[117] Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 34
[118] Lars Bo Langsted, Pter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 30
[119] Carsten Munk-Hansen: Retsvidenskabsteori (2014), p. 347
[120] Briefly discussed in the chapter on interpretation and construction in Danish law.

very common[121] in cases where there is an ambiguity in the statute's language; Danish courts do not preface every inquiry into legislative history with an argument for the existence of an ambiguity justifying the inquiry (US courts, conversely, appear to be quite reluctant to recognize terms as being ambiguous; this will be addressed briefly in the section on the rule of lenity in the chapter on nullum crimen sine lege).

3.4.2 Danish law and international law

Denmark is a dualistic state.[122] When an international convention is ratified, the convention does not automatically become a part of Danish law. Even if sufficiently clear, the articles of a ratified convention are not directly applicable and enforceable in national courts. Thus a ratified convention cannot become self-executing. For the convention to become a part of Danish law, the convention's articles must be incorporated into Danish national law by an act of Parliament.[123] Where domestic law requires no amended or new provisions to fulfill obligations under the convention, incorporation is not necessary as such (see below), but the convention does not become Danish law such that it could override conflicting laws.

Incorporation can take place in a couple of ways; by rewriting the convention into Danish law or by reference in law. Incorporation by reference is rare in Danish law.[124]

In some cases, there is a harmony of norms between the obligations set forth in the convention and the norms already present in national law. Harmony of norms is determined by comparing the substantive rules of the convention and the existing rules in national law.[125] In those cases, often no legislative steps are taken.[126] Such conventions, however, may be relied on in Danish courts and applied by Danish courts[127], presumably though only insofar as the language of the domestic rule leaves discretion to interpret in conformity with the international obligation.[128]

---

[121] Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 75
[122] Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 142
[123] Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 138, Morten Wegener: Juridisk metode (2000), p. 159 et seq., and Ole Spiermann: Moderne folkeret (2006), p. 169 et seq.
[124] Ole Spiermann: Moderne folkeret (2006), p. 171
[125] KBET 2014 no. 1546 Inkorporering mv. inden for menneskeretsområdet
[126] Ole Spiermann: Moderne folkeret (2006), p. 174
[127] KBET 2014 no. 1546 Inkorporering mv. inden for menneskeretsområdet, section 3 on the legal status of conventions in Danish law
[128] See also generally Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), p. 136 et seq.

Denmark, although technically a dualistic state requiring incorporation of treaties into national law, inherits monism with respect to certain treaties. When the Lisbon treaty entered into force, the European Union was granted the ability to act as a legal person (prior to Lisbon, only the European Community had legal personality). That is, the EU can enter into treaties that will legally bind all 28 member states. The EU is monistic and thus provisions in the treaties it enters can under certain conditions be automatically directly applicable without any further need for implementation. This monistic effect is passed on to the member states whether they are monistic or dualistic. For this self-executing effect to take place, a clear and precise obligation, the legal effect of and compliance with which does not presuppose acts of implementation, must be derivable from the provision's language, as well as the treaty's purpose and character.[129] This means that international law can enter the Danish legal system in two ways: 1) Through the EU with direct applicability and no requirement of incorporation into national law, and 2) through entering into treaties in Denmark's capacity as a sovereign state, requiring incorporation, i.e. the absence of direct applicability of the treaty in accordance with dualism.[130]

In summary, international law is only a source of law within the Danish legal system in so far as it is a part of Danish law. If it has not been incorporated, international law may affect the interpretation of existing Danish rules, as will be discussed in the chapter on interpretation and construction.

3.4.3 The Cybercrime Convention and Danish Law

Denmark signed the Convention on Cybercrime on 22 April 2003, ratified on 21 June 2005, and the Convention entered into force for Denmark on 1 October 2005.[131] According to Committee report no. 2002/1417, the existing substantive provisions in the Criminal Code fulfilled the treaty obligations to criminalize the acts in the Convention's articles 2-5.[132]

---

[129] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 222
[130] See Ulla Neergaard and Ruth Nielsen: EU-ret (2010), pp. 222-223
[131] Council of Europe's website, Chart of signatures and ratifications, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG, last retrieved on 31 January 2015.
[132] The remaining articles requiring criminalization in national law fall outside the scope for this dissertation for the most part.

It is unclear to which degree, if any, international obligations to criminalize can support or even compel courts to engage in a narrower reading of a national criminal statute, the language of which can support much broader readings. As mentioned in the section on Danish law and international law, it is not unusual to read Danish provisions in the light of international obligations. However, in the examples provided by *Spiermann*[133], Danish Criminal Code provisions, so far, only seem to have been limited in their scope in a balancing act with opposing actionable private rights, such as freedom of speech, rather than having their scope limited by reference to international obligations to criminalize acts, the scope of which is narrower than the existing criminal provisions that fulfil those obligations. The latter appears to be uncharted territory.

3.4.4 The ECHR and Danish law

Denmark signed the ECHR on 4 November 1950, ratification took place on 13 April 1953 with the Convention entering into force on 3 September 1953. Recall that ratification of a treaty is not sufficient for it to become a part of Danish law. The ECHR was not incorporated into Danish law until the passing of Act no. 285 of 29 April 1992. Up until the point of incorporation, Danish law is controlling. At the time of incorporation, the ECHR becomes a part of Danish law and is equal in authority to other Danish laws, with only the Constitution (Grundloven) ranking above it. Prior to its incorporation, the ECHR was an interpretational aid and courts could only interpret Danish laws in compliance with the ECHR insofar as the law in question left room for judicial interpretive discretion, and the resulting reading did not conflict with the national provision's language.[134]

3.4.5 The Council's Framework Decision 2005/222/JHA and Danish Law

One of the framework decisions adopted in the third pillar was Council Framework Decision 2005/222/JHA on attacks against information systems. Denmark decided to opt in on this framework decision and took steps towards implementation as early as 2002, with transposition in 2004, at the same time as Denmark incorporated the 2001 Council of Europe's Convention on Cybercrime.

---

[133] Ole Spiermann: Moderne folkeret, p. 166
[134] Ole Spiermann: Moderne folkeret (2006), pp. 165-166

As the European Community became the European Union, and the areas that prior to Lisbon had remained in the third pillar, were now part of the TFEU subject to the same institutional safeguards as the areas formerly residing in the first pillar. The protocol on transitional provisions, appended to the Lisbon treaty, provides some insight into what becomes of the legislative acts adopted within the scope of the third pillar. According to the protocol's article 9, the acts adopted under the TEU prior to Lisbon, remain in effect so long as these acts are not repealed, annulled or amended in accordance with the treaties. It follows from the protocol's article 10(1) that the Commission's competence to bring an action against a Member State for non-fulfilment of its treaty obligations (article 258 TFEU) does not apply with respect to old third pillar acts. Furthermore, the CJEU's limited competence with respect to third pillar acts remains the same as before Lisbon entered into force. Also in cases where Member States have given an article 35(2) declaration does the Court's pre-Lisbon competence remain the same. In article 10(2) of the protocol, it follows that if an act covered by article 10(1) is amended the Commission and the CJEU will have their post-Lisbon competences with respect to the act in question. However, article 10(3) of the protocol states that these transitional provisions cease to have legal effect five years after the Lisbon Treaty entered into force.

The Lisbon Treaty celebrated its fifth birthday in 2014, and thus the transitional provisions are no longer in effect. This effectively removes the leash off the CJEU and the Commission with respect to third pillar acts that are still in effect. Unlike the United Kingdom, Denmark had seemingly no reservations as to this consequence.

On 3 September 2013, the Framework Decision 2005/222/JHA was repealed and its replacement, Directive 2013/40/EU, was adopted. Denmark cannot opt-in on the directive (due to reservations), but rather, Denmark will continue to be bound by the Framework Decision with respect to the other Member States now operating under a directive that has expanded upon the older Framework Decision.[135]

[135] Commission Staff Working Document, Revised preliminary list of the former third pillar acquis, SWD(2014) 166 final. Dated 14 May 2014. See also Directive 2013/40/EU, preamble recital 34 ("Since the amendments to be made are of substantial number and nature, Framework Decision 2005/222/JHA should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive"), as well as article 9 of Protocol no. 36 on transitional provisions ("The legal effects of the acts of the institutions, bodies, offices and agencies of the Union adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the Treaties. The same shall apply to agreements concluded between Member States on the basis of the Treaty on European Union."), and cf. article 2 of

In light of the expiration of the transitional provisions must be assumed that the CJEU will have full jurisdiction, rather than the pre-Lisbon limited third pillar "opt-in jurisdiction"[136], over the Framework Decision. Similarly, the Commission can initiate infringement actions under article 258 TFEU after the expiration of the transitional provisions.

Article 2 of Protocol no. 22 on the position of Denmark states that none of the new legislative acts regarding police cooperation and judicial cooperation in criminal matters or the CJEU's interpretation of those legislative acts will be binding on Denmark or have any effect in Denmark. However, given the transitional provisions from which it appears that the CJEU now has jurisdiction over the Framework Decision (and that the Commission ostensibly can bring infringement actions against Denmark regarding the Framework Decision), and given that the language of many of the articles in the new Directive replacing the Framework Decision has largely been preserved, it is not unlikely that interpretation of the Directive might have effect on the interpretation of the Framework Decision anyway, regardless of article 2 in Protocol no. 22.

Protocol no. 22 ("acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon which are amended shall continue to be binding upon and applicable to Denmark unchanged.")

[136] Denmark did not opt-in on ECJ jurisdiction. See Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 281

4 INTERPRETATION AND CONSTRUCTION

This chapter addresses how the sources of law in chapter 6 are used in the various legal systems. This chapter is not intended to be a comprehensive description or analysis of rules on interpretation and construction[137], their theoretical background or their rationale. Rather, the chapter more particularly serves to explain how I use the sources of law in the rest of the dissertation, and show that the use is in line with the use in the particular legal system; regardless of whether opinion may divided within the legal system as to the use, such as is the case with using legislative history to discover legislative intent (be it general or specific intent) as an interpretative aid when applying e.g. statutes. The chapter is integral to the dissertation since the topic of the dissertation is the compounded vagueness of the law and the facts in hacking cases.

Interpretation in criminal law generally operates the same way as in any other area of law.[138] However, because of the serious implications of applying criminal law – that is, convicting a person and imposing a criminal penalty, such as imprisonment – interpretation of criminal provisions is subject to some limitations.[139] As will be accounted for in the chapter on the principle *nullum crimen sine lege*, the legislature cannot adopt too unclear criminal provisions and the courts cannot interpret criminal provisions in a way that is not reasonably foreseeable to those regulated or in a way that invites a high risk of arbitrary enforcement.[140]

Whether there is a legal basis for conviction for a criminal offense hinges on the statutory text. Interpretation of the statutory text is inevitable, as criminal statutes often describe categories of

---

[137] The title of this chapter implies a distinction between "interpretation" on the one hand, and "construction" on the other hand. The distinction is often made by commentators on US constitutional law. The distinction is generally not made with respect to Danish law, but it has been made with respect to EU law by Danish commentators. See e.g. Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 189 ("interpretation" is a reference to what in Denmark is known as "almindelig fortolkning" (determining the general meaning of a rule), and "construction" is a reference to what in Denmark is known as "subsumptionsfortolkning" (determining whether the rule can be applied to the facts of a particular case)). As explained by Nielsen and Tvarnø, the distinction becomes relevant in the Danish legal system by way of EU law; the CJEU is charged with the interpretation of EU law, whilst the member states are generally charged with its application. However, it is not uncommon that member state courts have phrased the question they submitted for preliminary ruling in such a way that the CJEU will also engage in construction (i.e. how the rule ought to be applied in the particular case).

[138] Trine Baumbach: Strafferet og menneskeret (2014), p. 72

[139] See Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 260 and see also generally on interpretation of criminal statutes in Wayne R. LaFave: Criminal Law (2010), p. 89 et seq.

[140] In Denmark's case too vague criminalizations contravenes article 7 of the ECHR whereas too vague criminalization in US law would render the statute void for vagueness (unconstitutional). See more in chapter on nullum crimen sine lege.

criminal conduct rather than describing every individual conceivable variation of the conduct within the category. Moreover, few words are entirely unambiguous and the objects a word describes may be few or many depending on the context (for example, when is a boat large enough to better be described as a ship?). The context in which the word appears will generally resolve ambiguity problems, but context does not necessarily delineate the precise boundary between which objects are covered by the word and which are not. The question of interpretation and construction in criminal law then involves figuring out whether the specific conduct at hand falls within the category of conduct described by a criminal statute. The answer to that question is not always obvious.

The language of the criminal statute, as enacted by the legislature, demarcates the outer limits of the statute's reach. Generally, the courts cannot add or detract elements from the statutory language. The figure below shows how conduct at the core is clearly covered by the scope, whereas the penumbra gives rise to increasing uncertainty as to the provision's application as the conduct moves further and further from the core, i.e. what is certainly covered by the provision's language.

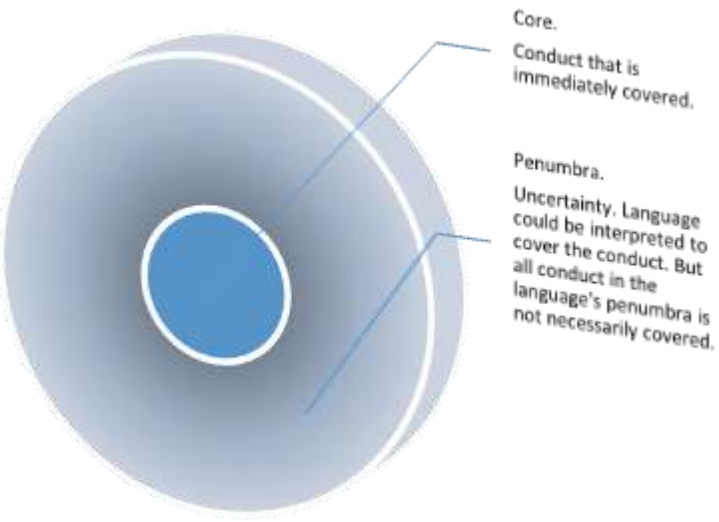


Figure 1 A visualization of the scope of any legal provision.

Where there is no doubt as to whether the conduct is covered by the statute, the conduct is likely a manifestation of the core conduct regulated. The core typically does not require interpretation as

such because the applicability of the statute with respect to core conduct is certain.[141] For example, application of an assault statute is certainly triggered when the defendant punches the victim and breaks the victim's nose. The conduct is a part of the core. But the language's meaning requires some stretching to cover, for example, the act of spitting on another person.[142] The conduct is a part of the penumbra, because it is uncertain whether the assault statute should apply to the act of spitting.

The penumbra ends where the language cannot be stretched further, and the word's usage, given the context, becomes more and more unusual.[143] Any conduct falling outside the outer limits of the penumbra can only be reached by the provision by analogous application, which is problematic in terms of foreseeability (as will be discussed in the chapter on nullum crimen sine lege) or the conduct cannot be reached at all by that particular provision.

Thus, whether conduct in the penumbra is covered by the criminal provision's scope is critical to whether there is a legal basis for a criminal conviction. Sometimes applying the provision to every conduct falling with the scope of the language may seem excessively harsh, and there are questions as to whether the legislature meant to criminalize that conduct.[144] Since clarification of the penumbra, and thus the reach of the criminalization, relies on interpretation and construction, it makes sense to explore the tools used by the courts to clarify the penumbra.

I will briefly examine interpretation in the following contexts (descending order): 1) International law (the general principles of interpretation in customary international law and interpretation of the ECHR), 2) EU law, 3) US law and 4) Danish law.

[141] See Alf Ross: Om ret og retfærdighed (2013), p. 162
[142] Spitting is for example covered by the Danish assault provision in the Criminal Code (section 244). The statutory language does not obviously include it, but the courts, through clarification in case law, have construed the provision as including spitting. See e.g. U 2005.2318Ø where a 4/2 majority voted to convict the defendant (and thus concluding that a single act of spitting on the victim fell within the scope of the assault statute). Two members of the court voted for acquittal arguing that the conduct in question was not covered by section 244.
[143] See Alf Ross: Om ret og retfærdighed (2013), p. 162 et seq.
[144] Wayne R. LaFave: Criminal Law (2010), p. 89

4.1 Interpretation in international law

4.1.1 Vienna Convention on the Law of Treaties

The Vienna Convention on the Law of Treaties[145] provides helpful guidelines on the interpretation of treaties in its section 3.

Article 31, GENERAL RULE OF INTERPRETATION

1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.

2. The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes:

(a) Any agreement relating to the treaty which was made between all the parties in connexion with the conclusion of the treaty;

(b) Any instrument which was made by one or more parties in connexion with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.

3. There shall be taken into account, together with the context:

(a) Any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions;

(b) Any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation;

(c) Any relevant rules of international law applicable in the relations between the parties.

4. A special meaning shall be given to a term if it is established that the parties so intended.

Article 32. SUPPLEMENTARY MEANS OF INTERPRETATION

Recourse may be had to supplementary means of interpretation, including the preparatory work of the treaty and the circumstances of its conclusion, in order to confirm the meaning resulting from the application of article 31, or to determine the meaning when the interpretation according to article 31:

(a) Leaves the meaning ambiguous or obscure; or

(b) Leads to a result which is manifestly absurd or unreasonable.

Article 33 of the Vienna Convention concerns different authoritative language versions of treaties. The article is omitted from this chapter.

According to the Vienna Convention's article 31 terms must be given their ordinary meaning, the ordinary meaning is tempered by the context in which the term appears (arguably as opposed to

[145] Vienna Convention on the Law of Treaties of 23 May 1969. Entered into force 27 January 1980.

applying purely any and all abstract definitions of the term, divorced from the context), and the ordinary meaning arrived should be in conformity with the treaty's object and purpose.[146]

Of specific interest for later discussion in this dissertation is the Vienna Convention's article 31(2)(a) and (b), that define as a part of the "context", along with the text, the preamble and annexes, agreements and instruments accepted by all parties in connection with the conclusion of a treaty. In all likelihood, the term agreement or instrument in this context covers explanatory reports accepted by all the parties in connection with the conclusion of Council of Europe treaties, e.g. the Convention on Cybercrime and its explanatory report.[147] The supplementary agreements and instruments "facilitate successful negotiation by clarifying sensitive diplomatic compromises that find imprecise expression within the original treaty text."[148]

Furthermore, article 31(3)(c) indicates that a treaty does not exist in a vacuum, but that other international law applicable to the parties are also part of the context.

Articles 31 and 32 are considered a codification of principles of interpretation in customary international law.[149] Article 31 prioritizes objective interpretation, and as article 32 indicates, recourse to supplementary means of interpretation such as preparatory works and circumstances of the treaty's conclusion leaves subjective interpretation secondary to objective interpretation.[150]

Article 31 describes both textual interpretation and teleological interpretation, but contains no information on when to apply one or the other.[151]

Article 32 comes into play where it might confirm the ordinary meaning arrived at through article 31 interpretation, or to determine the meaning of a term where the term is ambiguous or article 31 interpretation leads to manifestly absurd or unreasonable results.[152] During the drafters' discussion of preparatory works, delegates from less privileged countries expressed concerns over allowing

---

[146] See generally Ole Spiermann: Moderne Folkeret (2006), p. 125

[147] Interpretation contrary to what has been agreed upon in the reports may not be a good faith interpretation. The member states adopt the reports along with conventions, and thus, presumptively, adopt the meaning given to articles in the explanatory report unless there are indications to the contrary. See F.A. Engelen; Interpretation of Tax Treaties under International Law (2004), Doctoral Series, IBFD Publications, pp. 216-217. See also Barton Legum and William Kirtley: The Status of the Report of the Executive Directors on the ICSID Convention (2012), ICSID Review, p. 13.

[148] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 439

[149] Ole Spiermann: Moderne Folkeret (2006), p. 126

[150] Ole Spiermann: Moderne Folkeret (2006), p. 126

[151] Ole Spiermann: Moderne Folkeret (2006), p. 128

[152] See article 32 of the Vienna Convention on the Law of Treaties. See also Ole Spiermann: Moderne Folkeret (2006), p. 131

preparatory works to broadly influence interpretation and that it would favor wealthy countries with superior record-keeping, allowing them to disregard the text in favor of spurious unilateral interpretations based on materials unavailable to less privileged countries.[153]

4.1.2 Interpretation of the ECHR

The ECHR is an international treaty, which the European Court of Human Rights (ECtHR) is charged with interpreting and applying.[154] The rights contained within the ECHR are phrased in rather broad terms and they require interpretation and construction as to the extent of their scope when applied to facts. The rules of interpretation in the Vienna Convention on the Law of Treaties articles 31-33 have been regarded by the Court as codification of the principles of customary international law[155] and constituted the point of departure for the Court in its interpretation of the ECHR as an international treaty.[156] That is, the Vienna Convention's rules on interpretation have been used as guidelines by the ECtHR – even before the Vienna Convention came into force in 1980.[157] As noted by Jacobs, White and Ovey, the Court's interpretation of the ECHR follows two general themes. First, the interpretation of the Convention is teleological, inspired by the Vienna Convention's rule that allows for interpreting treaty terms in accordance with the treaty's object and purpose.[158] Second, the interpretation of the Convention as a living instrument (evolutive/dynamic interpretation).[159] The ECHR is a living instrument in that it is interpreted in light of present-day conditions rather than being interpreted in the light of conditions at the time of its adoption.[160]

One of the principles found in the Vienna Convention is article 31 (1), which calls for terms to be given their *ordinary meaning* in light of the *context* of the treaty and its *object and purpose*. The Court does reference dictionary entries[161] as an aid to determine the ordinary or natural meaning.[162]

---

[153] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 441. Note the US' subjective approach to treaty interpretation discussed later.
[154] Article 32 (1) ECHR. See also Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 64
[155] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 64 and 65-66, citing *Golder v. United Kingdom*, App. 13229/03, 29 January 2008, para. 62
[156] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 64
[157] The ECtHR did so in 1975 in *Golder v. United Kingdom*, Judgment of 21 January 1975, para. 29
[158] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 64 and Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 21. See also e.g. *Loizidou v. Turkey*, Judgment of 23 March 1995, para. 73.
[159] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 64
[160] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention (2010), p. 25 and see e.g. *Sigurður Sigurjónsson v. Iceland*, Judgment of 30 June 1993, para. 35
[161] Recall that dictionary entries provide the meaning of a word in the abstract.

The Court's use of context varies from just being the surrounding paragraphs to being the whole convention, including the preamble and protocols.[163] Generally, the Court will reject a restrictive interpretation of the ECHR's scope of application based on claims that suggest that the nature of the particular conduct that gave rise to the interference and the application to the Court.[164] However, see the chapter on nullum crimen sine lege (section on article 7 ECHR). The Court has repeatedly stated that the ECHR's purpose is to guarantee rights that are practical and effective, not merely theoretical or illusory.[165] This principle of effectiveness underlies the dynamic (evolutive) interpretation of the treaty.[166] Dynamic interpretation, however, does not permit the Court to read new rights into the ECHR that are not supported by the language, but it permits the Court to interpret existing rights in light of societal and political developments.[167] Thus, the text of the article places limits on how evolutive interpretation can get.

There is an important "exception" of sorts from the ordinary meaning rule, other than where the rule generates absurd or unreasonable results. What the ordinary meaning of a term is, from a general point of view, may differ between member states depending on their culture and legal system, and thus to avoid many different variations in how Convention rights' scopes are understood and applied at the national level, the ECtHR may give terms an autonomous meaning, specific to the Convention, to ensure uniform application throughout member states.[168] For example, the term "criminal offence" in article 7 ECHR is an autonomous term specific to the Convention, and not subject to member state idiosyncrasies. The autonomous meaning may be arrived at through comparative studies of the law in the states that are parties to the Convention.[169] Where a comparative approach does not yield much in terms of commonality, the Court gives member states flexibility with respect to their determining the scope of a certain term ("margin of appreciation"; usually in terms of whether an interference with a right is necessary, although the Court retains the

---

[162] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 68
[163] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 71
[164] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 24
[165] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 23 and see e.g. *Artico v. Italy*, Judgment of 13 May 1980, para. 33
[166] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 73. The interpretation rule on object and purpose in the Vienna Convention enabled this manner of interpreting the ECHR.
[167] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 72
[168] See Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 69
[169] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 69

power to review the exercise of discretion within the margin of appreciation).[170] This may also be the case where the particular subject matter is under development in the member states.[171]

Furthermore, the Court often seeks inspiration in other conventions.[172] Kjølbro argues that this may occur, because other conventions may contain more specific descriptions of norms than a generally phrased article in the ECHR, or for example, with respect to evaluating the risk of contradicting other applicable rules of international law.[173] It is important to keep in mind that other conventions are interpretative aids and not binding on the Court. It is of no particular importance that the member state before the Court is not bound by the convention being used as an interpretative aid.[174] Even non-binding documents such as recommendations from the Council of Europe's Committee of Ministers may be used as interpretative aids, e.g. because they may document a common understanding among the member states in terms of a particular subject matter.[175] Similarly, EU law may act as a source of inspiration, and the Court has also cited the Charter on Fundamental Rights in the European Union on occasion.[176] Case law from jurisdictions outside the member states has also been cited, e.g. cases decided by the Supreme Court of the United States.[177]

As indicated by the Vienna Convention articles 31 and 32, objective interpretation, that is, the more textual and teleological approach, takes priority over subjective interpretation involving preparatory works and discovery of the intent of the drafters.[178] Preparatory works rarely play any role in the ECtHR's interpretation apart from the cases where the reference to preparatory works is arguably only serving to bolster a decision already favored by the Court, or where the article in question is vague or ambiguous.[179] It is highly unlikely that the Court would give weight to preparatory works the content of which would militate in favor of a decision the Court finds undesirable.[180]

---

[170] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 69
[171] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 26
[172] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 28. Examples of conventions used are e.g. various Council of Europe conventions, UN conventions, the ILO conventions.
[173] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 28
[174] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 28
[175] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 30
[176] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 31 and see also e.g. *Goodwin v. United Kingdom*, Judgment of 11 July 2002, para. 100
[177] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 33 and see e.g. *James and others v. United Kingdom*, Judgment of 21 February 1986, para. 40
[178] Ole Spiermann: Moderne Folkeret (2006), p. 127
[179] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 22
[180] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 22

4.2 Interpretation in EU law

4.2.1 Teleological interpretation

Although the text is almost always the starting point of interpretation of EU law[181], the treaties' articles are oftentimes broad and vague and require interpretation in order to be applied to facts. In order to carry out its task the CJEU relies on the object and purpose of the treaties and the article in question to arrive at a result that comports with the purpose.[182] A written expression of the purpose need not exist, nor is it necessary that just because a purpose is explicitly stated in writing that it will exert decisive influence on the outcome of the case.[183] As a result, treaty provisions enshrining rights are interpreted broadly and the exceptions thereto are interpreted narrowly.[184] That is, an interpretation that effectively realizes the goals of the provision and the treaties is preferred.[185] With respect to secondary legislation, such as directives, the preamble is used in connection with teleological interpretation of the directive where provisions are vague or unclear, as the preamble generally states the object and purpose of the particular legislative act.[186] The CJEU often refers to preambles of secondary legislation when interpreting said legislation, although less frequently references preambles when interpreting the treaties.[187] [188] The CJEU's approach to teleological interpretation is almost always objective and on rare occasions subjective, in that preparatory work such as materials relating to the legislative history are rarely referenced.[189]

The CJEU's role does not involve application of a rule to the facts of the particular case before the member state court, which necessitated a preliminary ruling from the CJEU. Generally, it is up to the member state court to engage in construction, i.e. to apply the interpretation provided by the CJEU. However, it is not entirely uncommon for the CJEU to engage in construction, in particular when member state courts have phrased the question of interpretation submitted for preliminary

[181] Ulla Neergaard and Ruth Nielsen: EU ret (2010), p. 114
[182] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 124
[183] Ulla Neergaard and Ruth Nielsen: EU ret (2010), p. 117
[184] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 124
[185] Ulla Neergaard and Ruth Nielsen: EU ret (2010), p. 116
[186] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 124
[187] Ulla Neergaard and Ruth Nielsen: EU-ret (2010), p. 126
[188] According to the Vienna Convention's article 31, preambles are a factor in the interpretation of treaties.
[189] Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 124 and Ulla Neergaard and Ruth Nielsen: EU ret (2010), p. 120

ruling in such a way that ostensibly makes the process of interpretation inextricable from construction.[190]

4.2.2 General principles and doctrines

General principles play an important role in the interpretation and construction of EU law.[191] The principles have been developed by the CJEU, sometimes drawing inspiration from member states' legal systems, and some of the principles, such as the principle of proportionality, have been codified at the treaty level in later years.

The principle of supremacy of EU law (also known as the principle of primacy of EU law) was firmly established in 1964 by the CJEU (at the time, the ECJ) in *Costa v. ENEL*, case 6/64.[192] The supremacy of EU law is based on the member states' having ceded some of their sovereignty to the EU institutions and that the member states had committed themselves to observe community law.[193] Thus, if a conflict arises between EU law and national law, EU law is controlling. The principle is not limited to EU law that is directly applicable. The principle of indirect effect, or principle of consistent interpretation impliedly obligates national courts to give EU law priority over national law.[194]

Duty to loyal cooperation is found in article 4 TEU. This duty, along with the fact that directives are binding in terms of their aims, led the CJEU to develop the duty to interpret national law in conformity with EU law.[195] [196] This principle of consistent interpretation calls upon the national courts of the member states to ensure that the objectives of directives are achieved.[197] That is, EU law is applied indirectly by way of interpretation.[198] This means that national courts must interpret national law in light of a directive as far as it is possible, dependent on the extent of judicial

[190] Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 189 (the authors use the Centros case (C-12/97) as an example)
[191] See generally Takis Tridimas: The General Principles of EU Law (2006)
[192] See also *Van Gend en Loos* (case 26/62)
[193] Josephine Steiner and Lorna Woods: EU law (2009), p. 87. In *Costa v. ENEL*, the court cited *Van Gend en Loos*, as well as what are now article 288 TFEU and article 4 TFEU.
[194] Josephine Steiner and Lorna Woods: EU law (2009), p. 93
[195] This principle of consistent interpretation is also sometimes known as the principle of indirect effects. See Jospehine Steiner and Lorna Woods: EU law (2009), p. 124
[196] See e.g. *von Colson v. Land Nordrhein-Westfalen* (case 14/83).
[197] Josephine Steiner and Lorna Woods: EU law (2009), p. 125
[198] Josephine Steiner and Lorna Woods: EU law (2009), p. 125

discretion within the national legal system.[199] Even if the national law in question was not passed for the explicit purpose of implementing EU law, and when that legislation is older than the relevant EU law, the national courts are still under the duty to interpret the national law consistent with the objectives of the directive.[200] The principle of indirect effect also applies to framework decisions adopted under the old third pillar.[201]

There is, however, at least one express limitation to the principle of consistent interpretation. The limitation presents itself when the principle of consistent interpretation conflicts with the principle of legality.[202] Where a directive prescribes criminalization and criminal sanctions, and the directive has either not been implemented into national law, or has not been implemented correctly, namely, the national legal basis for crime and punishment is narrower than envisaged by the directive, the duty to interpret the national law consistently with the directive yields to the principle of legality. Hence, the exception to the principle of consistent interpretation applies in cases where the extensive interpretation, e.g. by way of analogy, of national criminal law in an effort to comply with EU law, would be to the detriment of the defendant. This limitation rests not on an imaginary "supremacy of national criminal law"[203], even though the criminality hinges on the scope of national criminal law. Rather the limitation follows from the principle of legality, which is "one of the general legal principles underlying the constitutional traditions common to the Member States"[204], and which is also enshrined in article 7 ECHR, article 15 ICCPR[205], and article 49 of the EU Charter. "It is a specific enunciation of the principle of legal certainty in substantive criminal law."[206] Thus, a national criminal provision cannot be interpreted extensively to achieve the purpose and object of a directive, if the legal basis in national law is narrower than that envisaged by the directive, or if the legal basis is absent all together.[207] Since framework decisions already lack the capability of direct effect, it is clear that they cannot serve as a legal basis for criminal sanctions. Transposition into national law is necessary. Since member states are obligated to interpret the

[199] Josephine Steiner and Lorna Woods: EU law (2009), p. 126. See also, Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 149. See the Court's ruling in C-105/03 *Pupino*.
[200] Josephine Steiner and Lorna Woods: EU law (2009), pp. 125-126, referring to *Marleasing SA v. La Comercial Internacional de Alimentación SA* (case C-106/89)
[201] Cf. C-105/03 *Pupino*. See Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), p. 148
[202] Opinion of Advocate General Colomer in Joined Cases C-74/95 and C-129/95 *X*, point 60
[203] Opinion of Advocate General Colomer in Joined Cases C-74/95 and C-129/95 *X*, point 76
[204] Opinion of Advocate General Kokott in C-105/03 *Pupino*, point 41
[205] The United Nation International Convenant on Civil and Political Rights
[206] Opinion of Advocate General Kokott in C-105/03 *Pupino*, point 41
[207] See Opinion of Advocate General Colomer in Joined Cases C-74/95 and C-129/95 *X*, point 74 and 75

implementing legislation consistently with the purpose and object of the framework decision, the principle of legality places a limitation on the "indirect effect" of a framework decision, just as is the case with directives. Ergo, directives and framework decisions cannot be relied on, in and of themselves, to establish criminal liability or aggravate criminal liability.[208] In those cases, the member state is obliged to act contrary to EU law with respect to the defendant, so as not to violate the principle of legality. Of course, the "exception" to the principle of consistent interpretation does not exempt the member state from liability for incorrect implementation or lack of implementation. Going forward, the member state is obliged to bring its national provisions into compliance with EU law, if it is proven the member state failed its obligation to implement EU law.[209]

In the converse situation, where the application of EU law results in a conduct not being unlawful, any national law criminalizing the conduct is inapplicable.[210]

4.3 Interpretation of US law

4.3.1 Interpretation of criminal statutes

US courts have often stated that if the statutory language is unambiguous there is neither the need to resort to interpretation nor the need to consult legislative history.[211] That is, there is no need to look outside the statutory text. This is called the plain meaning rule, and it generally applies insofar as the statute does not define the term in question, giving it a specific meaning other than the ordinary meaning.

However, to ascertain the plain meaning of the statutory language the courts frequently look to dictionary definitions.[212] Dictionary definitions give the reader an abstract meaning of the word that is looked up. The statutory text, which supplies the context in which the word appears, may limit its reach.[213] For example, the word "car" has a large penumbra in that it has many possible referenced objects; "car" may refer to a child's Matchbox car, a car for Barbie dolls, a four-person sedan that can act as a transportation for several people, a train car, and in its penumbra it might even refer to a tractor or an 18-wheeler, even though the language would be strained with respect to common usage in the last two examples. The particular expression in which the word appears provides context that limits the scope of

[208] See C-105/03 *Pupino* and C-80/86 *Kolpinghuis Nijmegen*
[209] See Opinion of Advocate General Colomer in Joined Cases C-74/95 and C-129/95 *X*, points, 76
[210] See Opinion of AG Colomer in joined cases C-74/95 and C-129/95 *X*, point 64, and joined cases C-358/93 and C-416/93 *Ministerio Fiscal v. Bordessa and others*
[211] Wayne R. LaFave: Criminal Law (2010), p. 90
[212] Wayne R. LaFave: Criminal Law (2010), p. 91, FN 11
[213] See Alf Ross: Om ret og retfærdighed (2013), p. 163

possible objects the word may reference. If the word "car" appears in a regulation on crash testing of passenger cars, relying on a plain meaning to include everything between Matchbox toy cars and tractors under the regulation's scope would be odd. Only the context narrows the word's possible references from the abstract to the specific. So establishing the plain meaning of a word in an expression with a very specific context by referencing abstract dictionary meanings appears somewhat odd in its pure form. The courts inevitably must engage in some form of construction to determine "plain meaning" of the statute, in that not the entire scope of a dictionary definition's possible references is included under a statute's scope. Choices must necessarily be made when determining what the plain meaning is, since the dictionary references only provide abstract definitions – not all of which are necessarily relevant to the context, nor is the scope of possible references of each dictionary entry necessarily relevant in the context.[214]

Even when language appears unambiguous, the courts have held that the language is ambiguous nonetheless, because the language is nonsensical, irrational or harsh.[215] In other cases, the courts have read "implied exceptions" into the statute.[216] The courts refer to these implied exceptions when applying the statute literally is undesirable if doing so leads to "injustice, oppression, or an absurd consequence. It will always, therefore, be presumed that the legislature intended exceptions to its language, which would avoid results of this character."[217] As an example, LaFave mentions a statute punishing speeding that would impliedly except from its scope the situation where a police officer exceeds the speed limit as he, in the course of his duty, follows a fleeing criminal in a high-speed pursuit.[218] That a criminal act was committed with good motives does not suffice for the act to be impliedly excepted. However, LaFave notes that most "implied exceptions" are more

[214] A critique of unprincipled reliance on dictionary entries can be found in Stephen C. Mouritsen: The Dictionary Is Not a Fortress: Defintional Fallacies and a Corpus-Based Approach to Plain Meaning (2011), Brigham Young University Law Review, p. 1915. Available at http://ssrn.com/abstract=1753333.

[215] Wayne R. LaFave: Criminal Law (2010), p. 91 (one of the examples cited by LaFave, p. 91, FN 13, is *Abuelhawa v. United States*, __ U.S. __, 129 S.Ct. 2102, 173 L.Ed.2d 982 (2009). The case involved a statute intended by Congress to punish facilitating drug transactions through use of a communication device. Violation of the statute constituted a felony. Another statute provided that those persons purchasing drugs thereby committed misdemeanors (first-time buyers), whereas those persons selling drugs committed felonies. The defendant in the case had used a phone to contact a seller with the aim of acquiring small quantities of drugs for his own personal use, something that would normally constitute a misdemeanor. However, the government had charged him with a felony due to his use of a phone to contact the seller with a view to buying the drugs. The simple usage of a phone subjected the defendant to up to twelve times the punishment compared to if the defendant had not used a phone. The Supreme Court disagreed with the government's "plain meaning" approach and stated "Congress used no language spelling out a purpose so improbable".)

[216] See Wayne R. LaFave: Criminal Law (2010), p. 91 et seq.

[217] Wayne R. LaFave: Criminal Law (2010), p. 91 (citing *United States v. Kirby*, 74 U.S. (7 Wall.) 482, 19 L.Ed. 278 (1869), noting though that the court need not have said anything about implied exceptions in this particular case, since the court could also have said that the action was not willful as required under the statute). Implied exception has also been used to explain "entrapment" ("defendant's nonliability where the police entrap him into violating the literal terms of a criminal statute"), Wayne R. LaFave: Criminal Law (2010), p. 92.

[218] Wayne R. LaFave: Criminal Law (2010), p. 92 (example derived from *State v. Gorham*, 110 Wash. 330, 188 P. 457 (1920))

appropriately treated as the general defense "necessity" – such as a starving person stealing food to save his own life.[219]

Furthermore, there are additional cases where the courts do not resort to "plain meaning". If a statute borrows a term from common law, the word is given its common law meaning unless the legislature has stated otherwise. Thus, the common law term is not given its "plain meaning" in the dictionary sense, but it is given its common law meaning.[220] There are instances where the statute's use of a common law term is not limited to the term's common law meaning.[221]

Legislative history can reveal legislative intent. As will be discussed below in the section on interpretation and construction in Danish law, legislative intent is an interpretative aid that is in no way binding upon the courts. Legislative history may contain conflicting statements or outdated considerations. Furthermore, not all judges are equally keen on using legislative history to resolve statutory ambiguities.[222] Especially in the context of criminal law where the public must be given fair notice as to which acts incur criminal liability, it would be problematic if legislative history could be used to expand the scope of criminal statutes beyond the statutory language.[223]

There is no disputing that the concept of legislative intent is one of fiction. The legislature is not a hive mind in the sense that every single person is in complete agreement with the purposes of the piece of legislation, that all involved have the same idea of what the language of the legislation means and the same ideas about whether any possible set of facts capable of falling within the scope of the language should trigger the application of the statute. Not only would such a concept of legislative intent presuppose a hive mind, it would also presuppose a hive mind capable of oracle-like clairvoyance and infinite wisdom, and thus capable of taking into account all possible future situations the language could apply to when it drafts and passes its semi-divine infallible text.[224]

There is, however, a difference between "general intent" (general legislative aim) and "specific intent".[225] Rather, the legislature is made up of people who frequently disagree about the details even when they agree on the bigger picture. In many instances, statutes may only represent the lowest common denominator of agreement capable of achieving

---

[219] Wayne R. LaFave: Criminal Law (2010), p. 92
[220] Wayne R. LaFave: Criminal Law (2010), p. 95
[221] See Wayne R. LaFave: Criminal Law (2010), p. 96. See also e.g. *Perrin v. United States*, 444 U.S. 37, 100 S.Ct. 311, 62 L.Ed.2d 199 (1979).
[222] Wayne R. LaFave: Criminal Law (2010), p. 99
[223] See Wayne R. LaFave: Criminal Law (2010), p. 99. See also *Crandon v. United States*, 494 U.S. 152, 160 (1990) ("Because construction of a criminal statute must be guided by the need for fair warning, it is rare that legislative history or statutory policies will support a construction of a statute broader than that clearly warranted by the text.")
[224] See criticism of "legislative intent" and canons of interpretation in Max Radin: Statutory Interpretation (1930), Harvard Law Review, Vol. 43, No. 6, pp. 863-885
[225] Such a distinction is made by e.g. Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819, p. 829 et seq.

majority consensus to secure the passing of the bill – and still that rests on the assumption that every member of the legislature read, understood and considered the consequences of passing the bill prior to voting in favor of it. Adding to that, draft bills are often written by people who are not part of the legislature. Furthermore, the legislative intent, if it can be determined with some certainty, is only a snapshot of the intent as it manifested itself under the circumstances at the time the statements were made. The future the legislature imagined may be vastly different when it arrived, and parts of the legislative intent would be inconsistent with the actual future conditions. Then why even entertain such a fiction as "legislative intent"? Because consulting legislative history and deriving some legislative intent need not reach the heights of "what did the legislature intend with respect to unforeseeable sets of facts", but rather deriving what interests the legislature sought to protect through criminal law (that is, deriving a broader, purpose-related intent, rather than intent as to a specific set of facts – which is arguably "less subjective" than asking what the legislature would have thought with respect to a specific case). Interpretation inevitably involves policy choices because it either leads to the inclusion or the exclusion of a set of facts under a statute that implements a policy – the question is only whose policy is being implemented, the court's or the legislature's? A purely "objective" approach to the interpretation of the statute, focusing solely on the statutory language, is in fact, arguably, even more subjective than resorting to a fictional legislative intent, because interpretation involves choices and the text itself does not necessarily provide those answers absent context.[226] Whether that context is the fictional legislative intent or the interpreting court's ideas of how the statutory language should be interpreted to solve the issue before it is a matter of choice. Since interpretation can never be wholly objective, the courts might have to accept that as long as the legislature is not an infallible oracle-like hive mind, they will have to make policy decisions within the margins of the ambiguity of statutory text – perhaps with some guidance from the general purpose-related thoughts expressed by the legislature where the text itself does not clearly reveal the protected interests.

The question of the legislature's ability to foresee possible constellations of facts has its appeal in some cases. The application of statutes to circumstances that the legislature never even conceived of, and could never have conceived of, just because the statute's language is capable of reaching the conduct, may result in absurd, unjust decisions along the way; especially if significant societal changes have taken place, such as is the case with the now pervasive use of computers and networks. Such decisions are in conformity with the rule of law, but the rule of law has never been and never will be "the rule of good law".

There are also situations where strict adherence to legislative intent is inappropriate. Perhaps, primarily the older the legislative history, from which intent is derived. Societal circumstances may have changed so drastically, and the intent may have been so specific as to the circumstances at the time, that the intent only partially has relevance for future application of the law, or no relevance at all. However, arguably, the age of legislative history is less relevant if it is simply a matter of determining the general legislative aim.

[226] The Danish legal theorist Alf Ross argued in his book "Om ret og retfærdighed" (2013), p. 189-190, that the objective approach to legislation, focusing only on the statutory text, was arguably more subjective than the subjective approach inherent in including legislative intent.

Like the usage of legislative history, the rule of lenity and others, the rule *ejusdem generis*, meaning "of the same kind", only applies where there is uncertainty, and furthermore, its application must not "defeat the obvious purpose of the legislation being construed."[227] The rule pertains to statutes that list certain objects and also include a "catch-all phrase". In this context, the ejusdem generis rule narrows the scope of the "catch-all phrase" to those objects that are within the same category as the specifically listed objects. The rule involves interpreting the statute in light of its context. Of course, the rule is only applicable where a category can be derived from the listed objects.[228]

The canon of avoidance, like the rule of lenity, is a tiebreaker in the sense that it mandates a specific result when the statute is capable of two or more constructions. The canon of avoidance, instead of favoring a specific party, disfavors constructions that raise serious constitutional questions. The court must thus choose the construction that avoids constitutional problems.[229]

Another important canon of statutory interpretation is the canon against superfluity. It means that every word of the statutory language should be given meaning and effect, if possible, to avoid making parts or all of the statutory text superfluous; that is, render whole or part of the language passed by the legislature without effect.[230]

4.3.2 US law and international law[231]

In the chapter on sources of law, it was explained that treaties entered into by the United States are at the same level in the hierarchy of sources of law as federal statutes. However, the apparent rule that treaties entered into by the US government share the second place with federal statutes in the sources of law hierarchy is only half the story. There are significant modifications to that rule. The Supremacy Clause of the US Constitution reads as follows: [232]

> "Treaties made, or which shall be made, under the Authority of the United States, shall be supreme Law of the Land."

[227] Wayne R. LaFave: Criminal Law (2010), p. 102
[228] Wayne R. LaFave: Criminal Law (2010), p. 102-103
[229] Wayne R. LaFave: Criminal Law (2010), p. 96-97
[230] *Hibbs v. Winn*, 542 U.S. 88, 124 S.Ct. 2276 (2004) at 101
[231] For the purposes of this dissertation, only treaties entered into on the basis of the United States Constitution, Article II, § 2. Executive agreements fall outside the scope.
[232] United States Constitution, Article 6, Clause 2

On its face, the Supremacy Clause seems quite clear on the status of international treaties in US law. However, early on in its case law, the United States Supreme Court differentiated between two types of treaties: First, treaties the authority of which equals federal legislation (self-executing), and second, treaties that require incorporation through legislative action by Congress and the President (non-self-executing). This means that only the first type of treaty is enforceable in US courts, whilst the second type of treaty is not.[233] Self-executing treaties have the force of law without requiring further legislative action.[234] Three reasons have been cited by courts as reasons for declaring a treaty non-self-executing: First, the treaty itself indicates that its provisions will not become effective unless legislative action is taken at the national level. Second, the Senate when giving its advice and consent advised that legislative action is needed. Third, legislative action is required as a matter of constitutional law.[235]

In a footnote in *Medellín v. Texas*[236], the Supreme Court "endorsed a "background assumption" against finding that treaties confer private rights or private rights of action, even when they are self-executing."[237] (citation omitted) The *Medellín* case raises doubts about the direct enforceability of treaties in US courts.[238] However, international treaties may be enforceable through other ways; 1) indirect enforcement, 2) defensive enforcement, and 3) interpretive enforcement.[239] These alternative enforcement options, the value of which rests on the assumption that the US is interested in fulfilling its international obligations[240], are more interesting and more relevant in the context of this dissertation, as the Convention on Cybercrime, which is central throughout most of the dissertation, confers no private rights to speak of nor are the substantive provisions self-executing.

---

[233] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, p. 52, citing Foster v. Neilson, 27 U.S. (2 Pet.) 253 (1829)
[234] Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 7
[235] Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 7-8
[236] 552 U.S. 491 (2008)
[237] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 53
[238] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, pp. 53-54
[239] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 76
[240] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 54

Indirect enforcement refers to a treaty that confers a right, but where the right is made actionable through national legislation.[241] This category of alternative enforcement comprises three subcategories; implementing legislation, section 1983 and habeus corpus. Neither this category nor its subcategories will be the subject of further discussion in this dissertation.[242] Generally speaking, the Convention on Cybercrime confers no tangible rights, but rather simply reminds the parties to ensure certain more or less unspecified safeguards under its domestic law, as well as it references international human rights obligations.[243] Even though the subcategory, implementing legislation, looks feasible on its face, no act of Congress implemented the Convention on Cybercrime into federal legislation. Rather, the non-self-executing parts of the Convention, namely those calling for criminalization, were found not to require implementing legislation as existing US law, combined with several reservations and declarations, was "adequate to satisfy the Convention's requirements for legislation."[244]

Defensive enforcement entails a private party, who is the target of a lawsuit or prosecution based on a statute that runs afoul of a treaty provision.[245] Defense enforcement is generally permissible even when the treaty does not confer private rights or provides a private right of action.[246] The cause of action is independent of the treaty.[247]

Interpretive enforcement involves the courts seeking inspiration or guidance in treaties when interpreting statutes.[248] As will be discussed further at a later point in this dissertation, an ambiguity brings interpretive canons into play[249]. This approach to enforcement of international treaties has the courts interpreting a statute so that it does not conflict with an earlier treaty. The approach is

---

[241] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 76

[242] See further elaboration on indirect enforcement in Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, pp. 77-83

[243] Council of Europe's Convention on Cybercrime (ETS no. 185), article 15

[244] Letter of Submittal to the Senate, Colin L. Powell, as well as Letter of Transmittal to the Senate, George W. Bush. Available at http://www.gpo.gov/fdsys/pkg/CDOC-108tdoc11/pdf/CDOC-108tdoc11.pdf. Last retrieved on 31 January 2015.

[245] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 76

[246] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 84

[247] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 84

[248] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 76

[249] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 88

applicable regardless of whether the treaty in question is self-executing or not.[250] When a conflict arises between a treaty and a statute, the Supreme Court has held that "[l]egislative silence is not sufficient to abrogate a treaty".[251] The Court refused to interpret a statute in a manner that would render a treaty unenforceable.[252]

Similarly, it follows from the *Charming Betsy*[253] canon that faced with two constructions, one that conflicts with international obligations and another that does not, the court should adopt the former insofar as it is a reasonable reading.[254] Furthermore, which will sound familiar to Danish jurists, a treaty will not be considered modified or set aside by later legislation unless doing so was the explicitly stated purpose of Congress.[255]

As far as interpretation of treaties goes, the US approach to treaty jurisprudence has been described by one commentator as "schizophrenic".[256] The apparent "schizophrenia" relates to the courts not consistently resorting to either a nationalist or internationalist approach to treaty interpretation. Until the early-to-mid twentieth century, the courts had seemingly consistently followed an internationalist approach, but thereafter started being challenged by nationalist views.[257] The mid-twentieth century saw the advent of the courts' adopting a private-law contract analogy.[258] That is, the courts would derive party intent based on all available evidence, rather than giving the treaty text priority[259] as generally required under customary international law (and codified in the Vienna Convention). One of the canons employed by courts, when approaching treaty interpretation from a

---

[250] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 88

[251] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 88, citing 466 U.S. 243, 252 (1984) (citing Weinberger, 456 U.S. at 32)

[252] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 88

[253] Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p 88. Also, Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 11 (citing *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804))

[254] Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014), p. 11 (citing *Murray v. Schooner Charming Betsy*, 6 U.S. (2 Cranch) 64, 118 (1804))

[255] *Cook v. United States*, 288 U.S. 102, 120 (1933). See Hathaway et al: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Law Review, vol. 37, p. 89

[256] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 499

[257] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 471

[258] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 472

[259] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 450

nationalist perspective, is the parole evidence rule under which the text is just "symbolic expressions of parties' actual intent."[260] The rule allows courts to liberally examine and consider other sources than the text, including purely domestic documents not included in the treaty's preparatory works, such as the internal treaty drafts of the State Department and executive branch's interpretation of the treaty, to establish a party's intent.[261] Such an approach may promote domestic interests[262] over the object and purpose of the treaty itself.[263] That is, subjective interpretation over objective interpretation – the opposite of what the Vienna Convention's articles 31 and 32 state.

The United States signed the Vienna Convention on 24 April 1970, but its ratification process stalled in committee, and the Senate has still not given its advice and consent as required for ratification.[264] Nevertheless, the State Department, as well as a number of lower federal courts, acknowledge many of the principles expressed in the Vienna Convention, including articles 31-33, as customary international law. [265] However, the Supreme Court has never applied the Convention.[266]

As discussed in the chapter on sources of law, the US are diligent users of RUDs[267] when ratifying treaties.[268] Whereas the Vienna Convention states that such RUDs must be accepted by both parties in order to be considered when interpreting the treaty, the US occasionally attaches RUDs

[260] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 451
[261] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 451
[262] Arguably, the extensive deference given by courts to executive interpretation of treaties may not help that matter. See generally Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2 on the extensive deference given to executive interpretation of treaties and brief comparison with the *Chevron* doctrine of interpretation in administrative law where deference is also given to agency interpretation. See also Restatement (Third) of Foreign Relations Law § 112 on the deference to executive branch interpretation (even in cases where the state is a party).
[263] See Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p.454
[264] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 443
[265] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 434 and 443. See also the State Departments website: http://www.state.gov/s/l/treaty/faqs/70139.htm
[266] Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 434 (it has only been cited in dissenting opinions)
[267] Reservations, understandings and declarations. Understandings typically do not change the treaty's substantive content. See Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 475
[268] The most notorious example is arguably the US RUDs to the ICCPR, which were numerous and subject to objections from treaty partners. For a discussion of the US RUDs to the ICCPR see Kristina Ash: U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence (2005), Northwestern Journal on International Human Rights, Vol. 3, Issue 1, Article 7

unilaterally, which nonetheless places constitutional[269] restraints on US courts as they have to honor even unilateral RUDs.[270] Such RUDs would require the US courts that generally do apply the Vienna Convention's interpretational principles, to depart from the Convention's objective approach to interpretation of treaties – regardless of whether the RUDs are unilateral or accepted by the other parties to the treaty.

4.4 Interpretation in Danish law

4.4.1 Interpretation of criminal statutes

As discussed below, in the chapter on nullum crimen sine lege, the Danish criminal code § 1 clearly expresses a criminal-law principle of legality. A legal basis must exist in a statute that describes both the criminal conduct and the penalty attached to it. If the existence or extent of a legal basis is too murky, courts will generally render a verdict of acquittal due to lack of a legal basis for conviction.[271]

In Danish law, descriptions of interpretation and construction can be divided into two categories: (1) Descriptions that relate to the conclusion, and (2) descriptions that relate to the premises of the conclusion.

Descriptions that relate to the conclusions are: (1) construction that clarifies the scope of the provision[272], (2) extensive construction, and (3) narrow construction. The second and the third both conflict with the natural meaning of the language of the provision in that an extensive construction may expand the scope outside the natural meaning of the language, and the narrow construction may reduce the scope of the provision even though the natural meaning of language allows for a broader reading.

---

[269] The Constitution ranks above treaties

[270] See Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44, no. 2, p. 476

[271] See chapter on nullum crimen sine lege

[272] The Gyldendal dictionary translates "præciserende fortolkning" as "strict construction". I will avoid using that translation, because the translation could cause confusion given later references to "the rule of strict construction" ("rule of lenity") in US law, which is a rule only applicable in criminal law and which dictates an outcome in favor of the defendant when applied. See note below. See also the section on rule of lenity in the chapter on nullum crimen sine lege.

Constructions that clarify the scope (*"præciserende fortolkning"*) are simply the results of choosing the most sensible reading out of two or more possible interpretations.[273] These types of constructions are always within the limits of the scope of the statutory text – never narrower or broader. They add precision to the scope of the statute.[274] Context is imperative to the understanding of the legal meaning of any rule. As explained before, most words are ambiguous and are capable of referencing a wide range of phenomena, which is also why context, not just of the word itself but the rule, is important, since words may reference different things in different contexts.[275] Thus, clarifying the scope is not about theoretically possible readings of the language, but plausible and reasonable readings of the language.[276]

The concept of extensive construction (*"udvidende fortolkning"*) is often used to refer to both those constructions involving analogous applications of statutes (constructions that are not supported by the language), and those constructions based on interpretations that go beyond the natural meaning of the statutory language but are technically supported by the language.[277] Broad readings that are compatible with the language of the scope are not "extensive constructions", since they do not exceed the limits of the natural meaning of the terms used in the statutory text even though such broad constructions may or may not appear harsh. The most drastic versions of extensive construction are those applications that are not supported by the statutory text at all but rest on analogies to the conduct described by that language. As discussed in the chapter on nullum crimen sine lege, the Danish criminal code § 1, allows for analogous applications of substantive criminal provisions to a limited extent. As explained later, in the chapter on nullum crimen sine lege, article 7 ECHR prohibits analogous applications of criminal provisions, which is why the Danish criminal code § 1 presumably may conflict with the analogy prohibition in article 7 ECHR.[278]

Narrow constructions (*"indskrænkende fortolkning"*), like extensive constructions, are not inherently compatible with the ordinary meaning of the enacted statutory text. Narrow construction

---

[273] There is no obligation in Danish law to choose the narrower reading in criminal cases, which is why I avoid translating "præciserende fortolkning" as "strict construction" in this context. "Præciserende fortolkning" is an entirely descriptive term in that the concept only implies that a choice has been made between two or more possible readings, but it is not a rule concerning, which alternative a court must choose.
[274] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 265
[275] See also Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), pp. 194-195. See also Trine Baumbach: Strafferet og menneskeret (2014), p. 72
[276] See also Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 195
[277] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 267. See also Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), pp. 196-197
[278] See e.g. Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), p. 30

means that the court has given the statute a narrower meaning than the natural meaning dictated by the statutory language. The Danish legal theorist, Alf Ross, defined two subcategories of narrow constructions: (1) Those cases where application of the provision would be superfluous with respect to achieving the purpose of the legislation[279], and (2) those cases where the conduct, although falling within the scope of the language, is atypical with respect to the core conduct prohibited by the statute. In both cases, the conduct has been exempted from the scope even though a literal reading of the language clearly indicates it should fall within the scope of the statute.[280] A narrow construction of a statute may also be warranted, even required, for example where the conduct clearly falls within the scope of the language of a criminal provision, but the conduct in question is also "protected conduct" under another rule (e.g. the conduct is covered by the right to free speech), thus creating an exception to the criminal provision in question; that is, two (or more) rules conflict.

In terms of separation of powers, both narrow and extensive constructions conflict with the ordinary meaning of statutory text enacted by the legislature by either giving the words a narrower or broader meaning than the word would ordinarily have. Thus, arguably, courts engaging in either type of construction technically usurp legislative power to some degree, as the power to criminalize and decriminalize conduct rests with the legislature.[281] However, only the latter is disadvantageous to a defendant in a criminal case and for that reason is suspect from a legal certainty point of view[282] in the sense that it reduces foreseeability.

As for approaches that relate to the premises of the conclusion, three categories are described in the legal theory: (1) Objective interpretation, (2) subjective interpretation, and (3) teleological interpretation.[283] These are all approaches that describe the "style of interpretation/construction" used to reach a result, irrespective of whether the end-result of the chosen approach can be described as an extensive, narrow or clarifying construction of the statute.

Objective interpretation is that which, when employed, relies only on the statutory text, or at least explicitly rejects relying on legislative history, and thus, rejects legislative intent as an interpretative aid.[284] The rationale for this approach is that the legislature only enacted the statutory text[285] – not,

[279] See also Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 196 (narrow purpose interpretation)
[280] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 266
[281] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 267
[282] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 267-268
[283] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 271 et seq.
[284] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 271

for example, committee reports, parliament debates and other materials related to the legislative history that may be used to discover legislative intent.

Subjective interpretation, on the other hand, involves openly considering legislative history materials relevant to discovering legislative intent in the court's effort to chart the intended meaning and thus the reach of the statute's scope.[286]

The choice between the objective and subjective approach to interpretation is not a quasi-religious commitment in the same way as it seemingly manifests itself in the US.[287] The choice may depend on which approach results in a more sensible application of the law in the case at hand.[288] However, interpretation can never be truly objective.[289] According to Ross, the judge's understanding of the law will always depend on his understanding of the social circumstances and purposes of the law. Ignoring other sources, including legislative history, leaves the judge with freer hands, and since statutory language does not really have any meaning without context, the objective interpretation is arguably more subjective than the subjective approach.[290] Both approaches add uncertainty, since both are subjective in different ways. The difference between the approaches is only whether legislative history (discovery of legislative intent) is considered or not.[291]

Legislative history, although often used in continental legal systems as an interpretational aid capable of having persuasive authority with respect to interpretation of statutes, it is important to remember that it does not have binding authority.[292] It is just one of many possible interpretational aids a court can consider when interpreting a statute. For example, if the legislative history is quite old[293] and the considerations made in committee reports refer to a society that has since undergone substantial changes[294], the legislative history as an interpretative aid has diminished value.[295]

---

[285] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 271
[286] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 271. See also Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 212
[287] Take for example Supreme Court Justice Antonin Scalia, who identifies himself as a textualist.
[288] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 271, citing Peter Blume: Lovfortolkning i retspraksis, p. 122
[289] Alf Ross: Om ret og retfærdighed (2013), p. 189
[290] Alf Ross: Om ret og retfærdighed (2013), p. 190
[291] Alf Ross: Om ret og retfærdighed (2013), p. 189
[292] Alf Ross: Om ret og retfærdighed (2013), p. 191
[293] See Ruth Nielsen and Christina D. Tvarnø: Retskilder og Retsteorier (2005), p. 221
[294] When reading about the *Liivik v. Estonia* case later on in the article 7 ECHR section of the nullum crimen sine lege chapter, consider, as a hypothetical scenario, the appropriateness of using the legislative history associated with a Soviet era provision as an interpretational aid when applying the provision in a market economy.
[295] See Alf Ross: Om ret og retfærdighed (2013), p. 191 et seq.

Canons of construction, like in US law, play a role in statutory construction in Danish law although they are rarely if ever discussed or mentioned in court decisions. For example, in case of conflicting statutes, the lex specialis (the specific governs the general) and lex posterior (the newer governs the older) canons may be applied to decide which of the conflicting statutes to apply.

Generally, if the meaning of the statute is clear with respect to its applicability in the case at hand, there is no need to resort to construction. That is, there is no need for construction where the conduct in question falls within the core of the statute, because in the core there is no uncertainty to clarify. In Danish law, an exception exist for some conduct that clearly falls within the scope of the provision's language. Conduct may exist that fall within the scope of the statutory language (even the core), but is nonetheless exempted from the scope, for example because although covered by the scope of the language, the conduct somehow differs from the essence of the crime. This principle of statutory construction, called *principle of material atypicality*, only applies when interpreting criminal statutes. The principle is explained further below in the chapter on authorization with respect to outsiders ("Without right" in the Danish Criminal Code § 263(2)).

It should be noted that oftentimes, Danish courts, although obligated to give reasons for decisions, do not articulate the precise reasoning, and thus, not articulating the exact method of reaching the decision in a case; i.e. why a specific interpretation was chosen over another, which rules of interpretation and construction it relied on in reaching its decision and so on are not recounted by the court. US courts are much more expressive in that respect.

4.4.2 International law as a source of law in Danish law

When a convention has been ratified but not incorporated into Danish law, it is not a source of law in the Danish legal system by the strictest definition. Should a conflict arise between a Danish law and such a convention, the convention cannot not override Danish law, as it is itself not Danish law. In the case UfR 2006.770H, the Danish Supreme Court held that treaties were not directly applicable in the sense that they could effect an override of Danish legislation.[296]

Even though a ratified treaty is not a part of Danish law as such, it is not without relevance. Treaties may act as a persuasive (meaning non-binding) authority when interpreting and construing Danish

[296] See Ole Spiermann: Moderne folkeret, p. 163. See also U2006B.187, Ole Spiermann: Lovgivnings tilsidesættelse og det retlige grundlag herfor: grundlov – menneskerettighedskonvention – traktat.

laws that in some ways relate to or overlap with a treaty.[297] In other words, international law may act as an interpretive aid. The outer limits of the possible influence of international law as an interpretive aid is that its influence can never support an interpretation of national law that clearly conflicts with the language of the national provision in question.[298] In other words, the extent of the interpretive influence is limited to reasonable readings of the national provision.

Should an incorporated treaty conflict with another domestic law, the incorporated treaty generally prevails, unless the legislature has clearly stated its intent to breach its international obligations under the treaty.[299]

Explanatory reports (non-binding)

An explanatory report is negotiated and adopted by the Council of Europe's expert committees and accompanies a Council of Europe treaty. The report provides clarifications on topics such as the purpose of the treaty, preparatory works, and interpretations of the articles in the treaty. The explanatory reports are non-binding, and do not provide an authoritative interpretation of treaty provisions although it may serve as an aid when applying treaty provisions.[300]

The explanatory report accompanying the Convention on Cybercrime was cited and referenced to rather extensively by the Danish Ministry of Justice in its comments on proposed legislation, although almost entirely regarding the procedural part of the Convention.[301] Explanatory reports have also been cited by the prosecution in at least one case, U 1986.200V where the court followed the interpretation in the explanatory report, and have also been cited in the cases U 2014.15Ø and U 2010.1035H. In both cases, the court relied on the interpretational guidelines in the explanatory reports.

[297] See Ole Spiermann: Moderne folkeret, pp. 161 et seq.
[298] Ole Spiermann: Moderne folkeret, p. 163
[299] U2006B.187, Ole Spiermann: Lovgivnings tilsidesættelse og det retlige grundlag herfor: grundlov – menneskerettighedskonvention – trakat, p. 193, referring to the Danish Supreme Court's decision in U2006.770H.
[300] See the Vienna Convention on the Law of Treaties article 31 (2)(a) and (b) regarding agreements relating to the treaty made between all the parties in connection with the conclusion of the treaty.
[301] LFF 2003-11-05 nr. 55

5 NULLUM CRIMEN SINE LEGE

This chapter covers the concept of nullum crimen sine lege. The chapter is not meant to be a comprehensive coverage of the principle of legality, e.g. its history etc. The chapter is mainly concerned with extensive interpretation of existing law – that is, judicial extension and gradual clarification, that is, construction of the scope of criminalization adopted by the legislature. Furthermore, the chapter will briefly address the limits on the legislature's power to criminalize conduct. The purpose of this is to examine the possibilities of limiting the effects of overcriminalization, or risk of overcriminalization, when the judiciary is entrusted with clarifying broadly worded and/or vague substantive criminal provisions.

The descriptions and analysis in this chapter serve to explore the potential impact of the nullum crimen sine lege principle on the broadly worded unauthorized access statutes. This will later serve to examine whether the principle is capable of placing some restraints on the courts as they construe these broadly worded statutes.

The principle of legality has its roots in ideas of separations of powers. The separation of powers was in turn spawned by a desire to prevent arbitrary use of power against citizens. From a criminal law point of view, as noted by Trine Baumbach, the separation of powers is imperative in the sense that if the legislature can make judicial decisions then the legislature is not bound by law, but is free to adjudicate arbitrarily, without any prior warning to citizens by way of pre-existing law.[302] As Peter Germer states, the separation of powers served to create a form of government where the power is balanced between the top government bodies, thereby protecting citizens from arbitrary use of power.[303] By requiring legislation prohibiting the particular conduct to pre-date a defendant's conduct, the defendant likely to be able to foresee the consequences of his conduct if he so desires.

One of the interesting questions pertaining to legislation in the context of this dissertation is: If a statute has been promulgated, but its language is so broad and/or vague that it leaves the statute capable of reaching any and all conduct and thus contains no particular criteria for its application that separates the legal from the illegal. In other words, even when legislation pre-dates a defendant's conduct the legislation may give no notice to the defendant, or solely gives notice in the

[302] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), pp. 30-31
[303] Peter Germer: Statsforfatningsret (2007), p. 13

form that anything one does can be framed as a violation of the statute should the government desire to do so, i.e. the citizen's only notice may be that the statute enables arbitrary enforcement.

5.1 Article 7 ECHR

The ECHR article 7 embodies one of the more important principles in the Convention, as article 15 (2) allows no derogation from article 7, including during time of war and public emergencies. It is an essential element of the rule of law.[304]

"ARTICLE 7

No punishment without law

1.

No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed.

2.

This Article shall not prejudice the trial and punishment of any person for any act or omission which, at the time when it was committed, was criminal according to the general principles of law recognised by civilised nations."

Article 7(1), first sentence, prohibits retrospective criminalization. The second sentence prohibits retrospective increase of punishment. The article is considered to embody both the principle of nullum crimen sine lege and the principle of nulla poena sine lege.[305] For conduct to be criminal, the law must define the crime and its associated penalty.[306] Not only must the law define the crime, it must do so clearly.[307]

[304] *C.R. v. United Kingdom*, Judgment of 22 November 1995, para. 32
[305] Trine Baumbach: Strafferet og menneskeret (2014), p. 127. See also *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 52.
[306] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 573
[307] *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 52

The rights in the Convention primarily regulate the relationship between state and individual and places some restraints on the state's power to intrude on aspects of an individual's life protected by fundamental rights enshrined in the Convention.

Article 7 ECHR must be interpreted and construed in accordance with its purpose in order to effectively guard against arbitrary prosecution, conviction and punishment.[308]

In its case law, the ECtHR has construed the article 7 ECHR protection against retroactive criminal laws so that the article imposes certain qualitative requirements on criminal legislation. This is the topic of the section and subsections below.

This dissertation only concerns itself with cases that are indisputably criminal cases and involve punishment/penalties for violation of criminal law rules. For that reason, it is not necessary to digress into analyzing when an offense is a criminal offense – thus, triggering article 7 ECHR – or when a penalty is a penalty within the scope of article 7 ECHR.[309]

5.1.1 Qualitative requirements: Accessibility and foreseeability

The qualitative requirements imposed on criminal law rules are those the Court has derived in case law from its interpretation of article 7 ECHR. As explained in the chapter on interpretation and construction, the Court interprets the ECHR in light of the purpose and object of the article it is interpreting. In order to make the rights effective in practice, sometimes they must be construed as containing requirements that are not expressed in the literal language of the article. "The guarantee enshrined in Article 7 […], which is an essential element of the rule of law, occupies a prominent place in the Convention system of protection, as is underlined by the fact that no derogation from it is permissible under Article 15 […] in time of war or other public emergency. It should be construed and applied, as follows from its object and purpose, in such a way as to provide effective safeguards against arbitrary prosecution, conviction and punishment."[310]

From the principle that a crime can only be defined by law, and the principle that a criminal provision cannot be extensively construed to the detriment of the defendant, e.g. by way of analogy,

---

[308] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 573, citing *Scoppola v. Italy (no. 2)* of 17 September 2009, para. 92

[309] An analysis of this was carried out in Trine Baumbach: Det strafferetlige legalitetsprincip (2008), chapter 7. See also Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010).

[310] *C.R. v. The United Kingdom* Judgment of 22 November 1995, para. 32

it follows that a crime must be clearly defined by law.[311] A criminal provision that suffers from vagueness issues to the extent that a person cannot reasonably foresee its application, or a criminal provision that is applied analogously, is arguably no different from retroactive criminalization, since in both situations there is an element of surprise that cannot reasonably be guarded against. As the US Supreme Court held on this point, there is no reason to allow the courts to do what the legislature could not; that is, criminalize retrospectively.[312]

The Court's test for whether a crime is defined by the law in the context of article 7, is largely the same as that which it applies to test the legal basis for interferences with the rights in articles 8 through 11 ECHR.[313] Under articles 8 through 11, the Court carries out a three-pronged test to evaluate interferences with said rights. First, the Court tests whether the interference is prescribed by law. This first prong largely equates to the entire article 7 test.[314]

"When speaking of "law" Article 7 alludes to the very same concept as that to which the Convention refers elsewhere when using that term, a concept which comprises statute law as well as case-law and implies qualitative requirements, including those of accessibility and foreseeability."[315]

The first prong, which corresponds with the article 7 test, is itself a three-pronged test known as the test of foreseeability.[316] First, there must be a legal basis in national or international law. Second, the law must be accessible. Third, the law must provide the regulated with reasonable foreseeability as to the consequences of his actions. The Court has labeled accessibility and foreseeability as qualitative requirements for the law.[317]

The concept of "law" not only comprises written law, but also unwritten law.[318] "[…][T]he Court has always understood the term "law" in its "substantive" sense, not its "formal" one. It has thus included both enactments of lower rank than statutes and unwritten law […]. In sum, the "law" is

---

[311] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 34. See also Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 579.
[312] See subsection on Legality in the section on Nullum crimen sine lege in the US.
[313] *Başkaya and Okçuoglu v. Turkey*, Judgment of 8 July 1999, para. 49
[314] Whereas the law must exist at the time of the conduct under article 7, under articles 8-11 it is the time of the measure constituting the interference that is relevant. See *Başkaya and Okçuoglu v. Turkey*, Judgment of 8 July 1999, para. 50.
[315] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para 77
[316] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 312
[317] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 312. See e.g. *Cantoni v. France*, Judgment of 11 November 1996, para. 29.
[318] Trine Baumbach: Strafferet og menneskeret (2014), p. 129

the provision in force as the competent courts have interpreted it."[319] The Court will generally "not question the national courts' interpretation of domestic law unless there has been a flagrant non-observance or arbitrariness in the application of the said provisions."[320]

Should the legal basis defining the crime and prescribing the punishment be absent seen from the point of national law, it is difficult to see how a state could defend its position and any defense on part of the Government will certainly fail.[321] If the rule has a legal basis in national law, the legal basis is subject to the qualitative requirements of accessibility and foreseeability to qualify as "law" within the context of the Convention.[322]

It is unclear whether accessibility and foreseeability are distinct requirements or more or less different shades of the same concept.[323] One commentator equates "accessibility" with "clarity".[324] Whether that characterization is accurate or not, I dare not say. However, the Court's case law seems to indicate that accessibility relates to whether the "law" has been promulgated[325] or is in some other way public – such as publication of the national courts' case law. In any case, it is unlikely that a conviction based on "secret law" not reasonably accessible to the public could pass a challenge under article 7.[326] It is seemingly rarely possible to distinguish between where the accessibility "analysis" ends and the foreseeability analysis begins, but in the very least, if a legal rule is not accessible, then its application and the effects thereof are hardly foreseeable either.

When the Court tests a national legal rule, such as a promulgated statute, it will, as mentioned, not test the statutory language, or other relevant source of law, on its face, but with its judicial gloss; i.e. how the courts have construed the language up until the time of the conduct.[327] Statutory language

---

[319] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 139
[320] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 84
[321] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 313. Also cf. *Vyerentsov v. Ukraine*, Judgment 11 April 2013, para. 67 ("The Court reiterates its earlier findings that although the offence of a breach of procedure for holding demonstrations was provided for by the Code of Administrative Offences, the basis of that offence, that is the said procedure, was not established in the domestic law with sufficient precision […]. In the absence of clear and foreseeable legislation laying down the rules for the holding of peaceful demonstrations, his punishment for breaching an inexistent procedure was incompatible with Article 7 of the Convention. In these circumstances, it is not necessary to examine separately whether the police orders could be considered lawful and therefore foreseeable from the viewpoint of the same provision.") The procedure, which the legal basis referred to and the violation of which was an element of the offense, did not exist.
[322] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 140
[323] Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR, p. 9
[324] Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR, p. 9
[325] See e.g. *N.F. v. Italy*, Judgment of 2 August 2001, para. 28 ("As regards the condition of accessibility, the Court considers that this requirement is satisfied because the law was public and accessible to the applicant.")
[326] Cf. *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 93. The Court is not referring to accessibility of the law, but facts relevant to the law in the form of access to a map attached to a 1953 report showing the demarcation of a military base, which the Court found that the defendant could not be expected to obtain in addition to the official map already in their possession.
[327] See *Kokkinakis vs. Greece*, Judgment of 25 May 1993, para. 40 (regarding "prescribed by law" in the context of article 9)

may therefore be unacceptably unclear on its face, but when read in concert with its judicial gloss, it may survive an article 7 challenge.

Foreseeability requires that "[a]n individual must know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it what acts and omissions will make him criminally liable and what penalty will be imposed for the act committed and/or omission. Furthermore, a law may still satisfy the requirement of "foreseeability" where the person concerned has to take appropriate legal advice to assess, to a degree that is reasonable in the circumstances, the consequences which a given action may entail."[328] Similarly, in *N.F. v. Italy*, the Court stated "that a law is "foreseeable" if it is formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct." [329] Arguably, foreseeability, in the ECHR context, is a kind of "lawyer's notice", rather than notice to the average individual, especially seeing as the average individual would likely lack the skills and knowledge to be able to read a legal text in the light of other sources of law that might cure the vagueness. Thus, rather than relying on whether the average individual can reasonably foresee the statute's application, the average individual may only need notice of when to seek legal advice. However, it should be kept in mind that the foreseeability requirement, and thus arguably the expectation of obtaining legal advice, varies depending on e.g. the characteristics and number of the regulated. That is, criminal provisions regulating certain types of business, rather than the general public, are subject to less stringent foreseeability requirements than criminal provisions that apply to every member of the public. See more below in the discussion of *Cantoni*.

The certainty, and thus the foreseeability, required is not absolute. Regardless of how clear the language, interpretation and construction is unavoidable.[330] As the ECtHR expressed it: "There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Again, whilst certainty is highly desirable, it may bring in its train excessive rigidity and the law must be able to keep pace with changing circumstances. Accordingly, many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice."[331] Article 7 does, therefore, not prohibit vague laws that

[328] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 140
[329] *N.F. v. Italy*, Judgment of 2 August 2001, para. 29. See also e.g. *Cantoni v. France*, Judgment of 11 November 1996, para. 35.
[330] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 141
[331] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 141

require interpretation, and the effect and reach of which becomes gradually apparent rather than being facially apparent. The Court only requires, with respect to such laws, that the gradual clarification of the rules prescribing criminal liability, "that the resultant development is consistent with the essence of the offence and could reasonably be foreseen."[332] It must be borne in mind that the Court "will not question the national courts' interpretation of domestic law unless there has been a flagrant non-observance or arbitrariness in the application of the said provisions."[333] (citations omitted) "The Court's role is confined to ascertaining whether the effects of such an interpretation are compatible with the Convention."[334] (citations omitted) This seems to be in congruency with the Court's statement that criminal law policy is a matter for the states. The Court will, therefore, not question whether a rule *should* apply to a particular set of facts, even if there are more than one plausible construction of the rule under national law and the chosen construction is harsher on the defendant (unless the conduct is protected as a substantive right under the Convention), but only whether the application of the rule was reasonably foreseeable and non-arbitrary.

5.1.1.1 Gradual clarification through case-law

In *Kokkinakis v. Greece*, the Court had before it a case concerning the Greek Constitution's proselytism prohibition. The applicant, a Jehova's witness, had been convicted of proselytism because he had attempted "directly and indirectly, to intrude on the religious beliefs of a person of a different religious persuasion from his own, [namely] the Orthodox Christian faith, with the intention of changing those beliefs, by taking advantage of [the person's] inexperience, her low intellect and naivety."[335] The Court set out to investigate whether the interference with freedom of religion under article 9 had been prescribed by law. As may be recalled, that inquiry is largely the same as that under article 7. The applicant had complained that there was a "logical and legal difficulty of drawing any even remotely clear dividing-line between proselytism and freedom to change one's religion […]." In other words, he argued that the prohibition was so vague that it was uncertain to which degree, if any, he could exercise his right to freedom of religion. In line with the Court's case law, the proselytism rule must be read in light of its judicial gloss. The Court stated, that "[i]n this instance there existed a body of settled national case-law. This case-law, which had

[332] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 141
[333] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 84
[334] *Liivik v. Estonia*, Judgment of 25 June 2009, para. 95
[335] *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 10

been published and was accessible, supplemented the letter of [the proselytism prohibition] and was such as to enable Mr Kokkinakis to regulate his conduct in the matter."[336] The Greek Supreme Administrative Court, in its 1953 definition of proselytism where it attempted to distinguish between "purely spiritual teaching" (legal conduct) and proselytism (illegal conduct), had written amongst other things: "Outside such spiritual teaching, which may be freely given, any determined, importunate attempt to entice disciples away from the dominant religion by means that are unlawful or morally reprehensible constitutes proselytism as prohibited by the aforementioned provision of the Constitution."[337] (The "dominant religion" requirement was later removed from the Constitution in 1975, and it then prohibited proselytism against all religions.) Recalling that the wording of many statutes is not absolutely precise, and that many laws are couched in vague terms to avoid excessive rigidity, the Court found that the proselytism prohibition fell in the category of vague laws, and was thus reliant on the practice of the national courts in clarifying the prohibition on a case-by-case basis, which the Court determined had occurred given the "well-settled case-law". The Court therefore found that the measure constituting the interference was prescribed by law. And thus, the Court, in its short article 7 analysis, simply referring to its article 9 analysis of whether the interference was prescribed by law, found that there was no breach of article 7.[338]

In *C.R. v. The United Kingdom* the applicant had been convicted of the attempted rape upon his wife, from whom he was separated at the time. The conviction was based on a statutory provision criminalizing rape. At the time, at common law, an exception was provided to the effect that a husband could not commit rape upon his wife as she had given consent to sexual intercourse at the time she entered into the marriage – so-called marital immunity. As unpalatable as such an immunity is, it nevertheless existed at the time of the applicant's conduct as a matter of law. Over the years, the domestic courts had created a number of exceptions to the immunity, thus allowing prosecution; however, none of these exceptions applied in the applicant's situation. Regardless, the national courts upheld the applicant's conviction and removed the marital immunity entire. The removal of the immunity defense occurred at a time when also the Law Commission recommended Parliament remove the immunity, but Parliament had not yet had a chance to act upon that recommendation. The Court found that there had been no breach of article 7. The Court reasoned that "[t]he evolution had reached a stage where judicial recognition of the absence of immunity had

[336] *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 40
[337] *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 17
[338] *Kokkinakis v. Greece*, Judgment of 25 May 1993, para. 52-53. The Court held that article 9 had been breached.

become a reasonably foreseeable development of the law." The Court continued: "The essentially debasing character of rape is so manifest that the result of the decisions of [the national courts] – that the applicant could be convicted of attempted rape, irrespective of his relationship with the victim – cannot be said to be at variance with the object and purpose of Article 7 (art. 7) of the Convention, namely to ensure that no one should be subjected to arbitrary prosecution, conviction or punishment. What is more, the abandonment of the unacceptable idea of a husband being immune against prosecution for rape of his wife was in conformity not only with a civilised concept of marriage but also, and above all, with the fundamental objectives of the Convention, the very essence of which is respect for human dignity and human freedom."[339] In *Pessino v. France*, a case about the continued construction activities of the applicant after the revocation of a previously issued construction permit, the Court found that the French court's departure from its precedent could not have been foreseeable to the applicant, and distinguished the case from *C.R. v. The United Kingdom* in stating that the debasing character of rape made the criminalization of the applicant's act foreseeable.[340] It is thus clear that the Court considered the removal of marital immunity as technically constituting retroactive criminalization, but due to the morally condemnable characteristics of the act in question, its criminalization should have been foreseeable despite of legal technicalities. Regardless of the despicableness of the applicant's conduct by any moral standard, and the obvious need to remove the marital immunity, the Court's reasoning leaves the taste of the rationalizing of a conclusion that, in essence, allows for a form of retroactive punishment of conduct, which is clearly highly undesirable, and yet not subject to punishment under the national law without retrospective removal of the marital immunity. The national courts adopted the marital immunity, albeit in a different time, but still had not abolished it in the late 20th century. In fact, the national courts had always recognized some form of immunity in these kinds of cases up until the applicant was convicted.[341] The legislature had also failed to act to abolish the marital immunity altogether. According to another commentator, had the applicant sought legal advice prior to his conduct, the advice would most likely have warned of the imminent reform, but maintained

[339] *C.R. v. The United Kingdom*, Judgment of 22 November 1995, para. 41-42
[340] *Pessino v. France*, Judgment of 10 October 2006, para. 36 ("A cet égard, la Cour considère que la présente affaire se distingue clairement des arrêts S.W. et C.R. c. Royaume-Uni (paragraphe 19 ci-dessus), dans lesquelles il s'agissait d' un viol et d'une tentative de viol de deux hommes sur leurs femmes. La Cour avait pris soin de noter dans ces arrêts (§§ 44 et 42, respectivement) le caractère par essence avilissant du viol, si manifeste que la qualification pénale de ces actes, commis par des maris sur leurs épouses, devait être regardée comme prévisible et non contraire à l'article 7 de la Convention, à la lumière des objectifs fondamentaux de celle-ci, "dont l'essence même est le respect de la dignité et de la liberté humaines".")
[341] *C.R. v. The United Kingdom*, Judgment of 22 November 1995, para. 19

that marital immunity was still valid law.[342] It is odd that, ostensibly, the citizen must assume the risk for the state's failure to act upon a legal situation that long since had become socially unacceptable. Of course, one the one hand, it would be regrettable from a moral standpoint and offensive to the idea of justice for the woman involved if the applicant had benefitted from the state's failure to protect married women in such an egregious manner. However, on the other hand, the decision not to allow the applicant to benefit from the state's failure, arguably, comes at the price of the introduction of a degree of arbitrary enforcement of article 7 itself, by declining to find a violation based on moral grounds rather than legal arguments. There are negative implications involved no matter which alternative the Court had chosen. However morally correct I think the decision is, I am not entirely convinced it was the correct decision from a strict legal point of view, since the Parliament could have resolved the issue with prospective effect rather than the courts resolving the issue with retrospective effect for the applicant.[343]

Whereas *C.R. v. The United Kingdom* involved retrospective revocation of an exemption from criminal liability, the *Cantoni* case involved the question of the legislature's use of a broad category in a criminal provision, and the applicant's complaint that the scope of the category was subject to lack of clarity and arbitrariness. In the *Cantoni* case, the legal provision in question targeted "medicinal products" as a category, rather than providing an exhaustive list of products considered "medicinal". The domestic courts had, over time, included in the category of medicinal products everything from actual pharmaceuticals to Vitamin C, 70% strength alcohol and mineral supplements. The Court, stated in *Cantoni* that "[w]hen the legislative technique of categorisation is used, there will often be grey areas at the fringes of the definition. This penumbra of doubt in relation to borderline facts does not in itself make a provision incompatible with Article 7 (art. 7), provided that it proves to be sufficiently clear in the large majority of cases. The role of adjudication vested in the courts is precisely to dissipate such interpretational doubts as remain, taking into account the changes in everyday practice."[344] The Court, concluded that in the *Cantoni* case, the legal provision in question did pass article 7 muster; in light of the case law available at

[342] Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 10. Murphy furthermore cites another commentator criticizing such a profound change carried out by the judiciary rather than the legislature. (Murphy, footnote 60, referring to R Beddard: The rights of the "criminal" under Article 7 ECHR (1996)).
[343] See also criticism of the judgment in Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 302-303
[344] *Cantoni v. France*, Judgment of 11 November 1996, para. 32

the time, the statutory rule was sufficiently clear.[345] Furthermore, the Court stated that it could not express its "view on the appropriateness of methods chosen by the legislature of a Contracting State; its task is confined to determining whether they are in conformity with the Convention."[346] In light of the case law at the time, which also showed that the domestic appellate court had never upheld a lower court's finding that parapharmaceutical-type product fell outside the scope of the provision,[347] Mr Cantoni ought to have known that "he ran a real risk of prosecution for unlawful sale of medicinal products."[348]

The degree of foreseeability required is not the same in all cases and varies dependent on at least three factors. It depends to a considerable degree on the text of substantive provision in question[349], the area of law in question[350], as well as the number and characteristics[351] of those regulated by the provision in question.[352] The above reference to the need for a person to seek legal advice is particularly pertinent "in relation to persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation. They can on this account be expected to take special care in assessing the risks that such activity entails."[353]

5.1.1.2 Extensive interpretation and analogy

In *Kokkinakis*, the Court made the important statement that article 7 not only embodies the principle that only the law can define crime and penalties, but also the principle that the criminal law must not be *extensively construed to an accused's detriment, for instance by analogy*. From this follows, the Court wrote, that an offense must be *clearly* defined in law. An offense is clearly defined in law "where the individual can know from the wording of the relevant provision and, if need be, with the assistance of the courts' interpretation of it, what acts and omissions will make him liable."[354] The clarity requirement is thus not solely aimed at the language of the rule, but rather at the clarity of the law as it has been interpreted by courts. This section is dedicated to the cases where the reading of

[345] *Cantoni v. France,* Judgment of 11 November 1996, para. 32
[346] *Cantoni v. France,* Judgment of 11 November 1996, para. 33
[347] *Cantoni v. France*, Judgment of 11 November 1996, para. 34
[348] *Cantoni v. France*, Judgment of 11 November 1996, para. 35
[349] *Cantoni v. France*, Judgment of 11 November 1996, para. 35
[350] Laws on terrorism as made clear in *Başkaya and Okçuoğlu v. Turkey*.
[351] Laws applicable to business professionals such as in *Cantoni v. France*.
[352] *Cantoni v. France,* Judgment of 11 November 1996, para. 35. See also Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 582.
[353] *Cantoni, v. France,* Judgment of 11 November 1996, para. 35
[354] *Kokkinakis v. Greece,* Judgment of 25 May 1993, para. 52

the law is unreasonable because the interpretation goes beyond the limits of the provision's language.

It is clear from *Kokkinakis* that laws can be quite vague without running afoul of article 7.[355] However, the Court does not tolerate any degree of vagueness, including unforeseeably expansive interpretations that go beyond the letter of the law.

In *Liivik v. Estonia*, the Court held that article 7 had been breached. The case concerned an applicant who had served as acting Director General of the Estonian Privatisation Agency. He had decided that a public limited company in possession of the Estonian railways should be privatized. The Public Prosecutor's Office, as well as a number of other public officials, had on several occasions expressed the opinion that the privatization was lawful. However, the Public Prosecutor's Office later drastically changed its opinion and the applicant was charged with and convicted of misuse of an official position and thereby causing *risk* of significant damage, and in doing so allegedly had caused significant *moral* damage to the interests of the state. His conviction was based on a Soviet era provision, now being applied in a market economy. However, according to the provision's language, the risk had to have materialized, as the wording of the provision did not allude to risk sufficing as a trigger for its application.[356] The applicant was also obligated to privatize the company, and thus, had to balance risks as a part of his position at the privatization agency.[357] The Court, thus, held that it was not foreseeable to the applicant that his acts would trigger the application of the provision in question. Particularly troubling was the interpretation of "significant damage" as including "significant moral damage", such as not acting in compliance with a "general sense of justice" (and the what made damage significant was that the applicant was a high-ranking state official) – a rather open-ended concept. As the Court noted, the domestic court exercised its discretionary judgment, when interpreting "moral damage", in such a way that it was not susceptible to proof.[358] The Court noted that "[i]t appears that the fact of an alleged violation of law by the applicant in itself served as an irrebuttable presumption that he had caused moral damage to the interests of the State. So broad an interpretation could, in principle, render any breach of law

[355] However, the breadth of a vague provision that constitutes an interference with protected conduct may be in violation of article 8-11, because the provision causing interference will fail the proportionality test if it causes greater interference with protected conduct than necessary to pursue a legitimate aim.
[356] *Liivik v. Estonia*, Judgment of 25 June 2009, para. 99
[357] *Liivik v. Estonia*, Judgment of 25 June 2009, para. 99
[358] *Liivik v. Estonia*, Judgment of 25 June 2009, para. 100

a criminal offence within the meaning of [the provision in question].”[359] The Court further stated that “the interpretation and application of [the provision] in the present case involved the use of such broad notions and such vague criteria that the criminal provision in question was not of the quality required under the Convention in terms of its clarity and the foreseeability of its effects.”[360] The Court thus found that article 7 had been breached.[361] The *Liivik* case, compared with *Kokkinakis* and *Cantoni* for example, goes to show that it seemingly takes an exceptional degree of vagueness before article 7 is violated. *Liivik* contained what could arguably be labeled a “compounded breach”. Not only was the provision extensively interpreted to include the mere risk of damage where the language only reasonably supported a reading requiring damage to have occurred, but the interpretation of “damage” as also meaning “moral damage” made the provision’s application impermissibly vague as well as being extensively interpreted to the detriment of the applicant, such that he could not reasonably foresee being prosecuted for a violation of the provision. A vague concept (e.g. moral damage) cannot be cured by interpreting it with reference to another vague concept (e.g. the general sense of justice).[362]

In *Başkaya and Okçuoğlu v. Turkey* the applicants had been charged and convicted under the Turkish Prevention of Terrorism Act. The first applicant had written an academic essay published as a book critiquing the official ideology of the state with respect to Kurdistan. The second applicant owned the publishing house, which published the book. The first applicant was charged with “disseminating propaganda against the indivisibility of the State”, and the second applicant was charged under a provision targeting the publishers of such propaganda. However, the punishment applied to the applicant targeted editors, instead of the more lenient punishment applicable specifically to publishers that only allowed imposition of fines upon a publisher.[363] To the applicants’ complaint of vagueness of the notion of “dissemination of propaganda against the indivisibility of the State”, the Court responded with reference to its case law that “Article 7 embodies, *inter alia*, the principle that only the law can define a crime and prescribe a penalty (*nullum crimen, nulla poena sine lege*) and the principle that the criminal law must not be

[359] *Liivik v. Estonia,* Judgment of 25 June 2009, para. 100
[360] *Liivik v. Estonia,* Judgment of 25 June 2009, para. 101
[361] It ought to be noted that the national Parliament and Supreme Court had already cast doubt on the conformity of the “significant moral damage” element, as well as the broad interpretation leading to the inclusion of mere risk of significant damage, with the nullum crimen sine lege principle. See *Liivik v. Estonia*, Judgment of 25 June 2009, para. 103.
[362] See also brief commentary in Trine Baumbach: Strafferet og menneskeret (2014), pp. 144-145
[363] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 13 and 27

extensively construed to an accused's detriment, for instance by analogy. From these principles it follows that an offence and the sanctions provided for it must be clearly defined in the law."[364] On a side-note, it is unclear whether the Court's addition of "*inter alia*" to its boilerplate-like paragraph on the substance of article 7 makes any tangible difference other than just keeping the door open for other possible applications.[365] Regarding the vagueness of the law, the Court noted that "in the area under consideration it may be difficult to frame laws with absolute precision and that a certain degree of flexibility may be called for to enable the national courts to assess whether a publication should be considered separatist propaganda against the indivisibility of the State."[366] The Court, furthermore, stated that contrary to the applicants' claims, the terrorism provision did not confer over-broad discretion on the national court in interpretation the scope of the offense.[367] It, thus, in the article 7 context, found that both applicants' convictions were compliant with article 7. However, the Court found that the penalty imposed on the second applicant, the publisher, was based on extensive construction, by analogy, of a *lex specialis* rule concerning editors that allowed the imposition of a prison sentence rather than applying the rule regarding publishers allowing only for a fine. The prison sentence applied to the second applicant was therefore in violation of the principle nulla poena sine lege embodied in article 7.[368] [369]

5.1.1.3 Quality of law?

In *Kafkaris v. Cyprus*, the applicant had been convicted in 1989 of three premeditated murders (contract killing) he committed in 1987. Under the national criminal code, premeditated murder carried with it a mandatory sentence of life imprisonment. The concept "life imprisonment" was not defined by the criminal code. In the applicant's case, the trial court, following a prior decision, had stated that "life imprisonment" meant imprisonment for the remainder of the applicant's natural life. Two regulations had been adopted in 1981 and 1987 on the basis of law on prison discipline, which were meant to regulate the execution of sentences, including remission of sentences for good behavior. In the 1987 regulation, the term "life imprisonment" was defined as twenty years

[364] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 36
[365] Perhaps the Court's introduction of "quality of law" requirement in *Kafkaris* is an example of what "*inter alia*" could mean, but that is just guesswork at this point.
[366] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 39
[367] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 39
[368] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 42
[369] Both convictions were found incompatible with article 10 ECHR. *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 67.

imprisonment. Taking remission based on good behavior into account, the convicted person would be scheduled for release after serving fifteen years. Such a scheduled release date would be noted in the prisoner's file. When the applicant was admitted to serve his sentence, he was given written notice of a scheduled release date of 16 July 2002. Due to a disciplinary infraction the release date was delayed till 2 November 2002. In 1992, the Supreme Court declared the regulations unconstitutional and *ultra vires*. The regulations were then repealed in 1996.

Although rules concerning the execution of sentences generally does not fall within the scope of article 7, the Court observed that the line between definition of sentences and rules on the execution of sentences is not always clear.[370] Moreover, the Court stated that in the present case it was clear that "in reality the understanding and the application of these Regulations at the material time went beyond [the execution of penalty]. The distinction between the scope of a life sentence and the manner of its execution was therefore not immediately apparent."[371] The national courts did not clarify the distinction until after the time of the applicant's conduct, and also, that in both the 1992 Supreme Court case, and the applicant's case, the prosecution appeared to take the view that a life sentence equated twenty years imprisonment.[372] However, the Court did not take the view that a heavier penalty had been imposed retrospectively, because the criminal code did not define life imprisonment to mean twenty years imprisonment.[373] The Court thus held that there had been no violation of article 7 – in that respect.

Perhaps surprisingly, the Court added that the present case was rather a question of "quality of law".[374] "In particular, the Court finds that at the time the applicant committed the offence, the relevant Cypriot law taken as a whole was not formulated with sufficient precision as to enable the applicant to discern, even with appropriate advice, to a degree that was reasonable in the circumstances, the scope of the penalty of life imprisonment and the manner of its execution."[375] On that basis, the Court held that there had been a violation of article 7.[376]

Even though the Court found a violation with respect to "quality of law", the Court noted that it was a consequence of the change in the prison law that the applicant no longer had a right to remission

[370] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 142
[371] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 148
[372] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 148
[373] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 149
[374] *Kafkaris v. Cyprus*, Judgment of 12 February 2008, para. 150
[375] *Kafkaris v. Cyprus*, 12 February 2008, para. 150
[376] *Kafkaris v. Cyprus*, 12 February 2008, para. 150

of his sentence that matter related to the execution of his sentence as opposed to the penalty imposed in him, namely life imprisonment.[377] The Court's finding of a violation brought with it no remedy for the applicant.

The "quality of law" requirement, although it appears new, is likely only a mix of accessibility and foreseeability rather than a new requirement under article 7.[378]

Perhaps the Court's reasoning can be restated in the following way. Because there was no clear right to a maximum of twenty years of imprisonment when sentenced to life imprisonment at the time of the applicant's sentencing, although there were arguments in favor of it, then the Court could not clearly establish that a retrospective increase in penalty had occurred. However, just because there was not enough clarity to establish definitively that the applicant was entitled to be released after twenty years' incarceration, did not mean that the unconstitutional regulations had not injected enough uncertainty that the law at the material time required clarification; especially when seen in light of the trial court's specification of life imprisonment in its literal sense and the legal basis for that penalty in the criminal code. The confusion was likely only compounded by the fact that the regulations not only over-stepped the limits of its enabling provision in the primary law, but also apparently directly contradicted a provision in the primary law, which indicated that prisoners serving life sentences were not eligible for remission of their sentence except where the Governor saw fit to release them on license. In other words, there was arguably not enough certainty to legitimately rely on a maximum of twenty years' incarceration when committing an act subject to life imprisonment, and the criminal code's lack of definition of life imprisonment left room for the possibility that life imprisonment meant exactly that and nothing else. Perhaps this is an indication that uncertainty need not reach the levels of retroactivity of criminal laws to fail under article 7 scrutiny, but could fail due to bad draftsmanship, e.g. where the state of the law at the time of the conduct is so unclear and/or contradicting that it is not determinable with an acceptable degree of certainty. After all, for the Court to be able to determine whether a law has been applied retrospectively, it needs to be able to determine what the law was at the time of the conduct in the first place, and whether the applicant's conviction and penalty were consistent with that law. In *Kafkaris* there was no *determinable* retroactive increase in punishment.

---

[377] *Kafkaris v. Cyprus*, 12 February 2008, para. 151

[378] Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 12

In *Camilleri v. Malta*, the applicant had been convicted of possession of illegal substances with the intent to supply. Under Maltese law, the offense with which the applicant had been charged and convicted was clearly defined in law. However, while the law defined the punishment for such an offense, the law provided two different possible punishments based on whether a defendant was tried before the Court of Magistrates or before the Criminal Court. Before the former, the punishment was six months to ten years, and before the latter, four years to life imprisonment.[379] Clearly, the punishment for the offense had a legal basis. Even so, the law must also be accessible and the consequences of one's actions reasonably foreseeable. The Court proceeded to determine whether, in particular, the foreseeability requirement was satisfied, seeing as the choice of jurisdiction – a decision made by the prosecutor – affected the possible penalty applicable.

The Court observed that the law did not provide any guidance with regard to which penalty bracket would be applied to the applicant, and he would only become aware of the applicable bracket when charges were brought against him.[380] This would depend entirely on the Attorney General's discretion to choose the jurisdiction. The Court further noted, in the light of the case law provided to it, that the Attorney General's decisions were at times unpredictable.[381] Even if the applicant had sought legal advice, the Court averred, the applicant would not have been able to know which bracket would be applied to him, because "the decision was solely dependent on the prosecutor's discretion to determine the trial court."[382] The law did not specify which criteria were relevant to the prosecutor's decision, and the no other guidelines existed either. The law thus did not provide any degree of precision with respect to when the application of which bracket would be triggered, because the law did not contain any guidelines as to what constituted a less serious offense and a more serious offense.[383] The Court thus noted that "[t]he Attorney General had in effect an unfettered discretion to decide which minimum penalty would be applicable with respect to the same offence. The decision was inevitably subjective and left room for arbitrariness, particularly given the lack of procedural safeguards."[384] The chosen trial court would thus be bound by the prosecutor's decision in that it could not, regardless of the circumstances of the case and regardless of any concerns a judge might have about the use of discretion, impose a lesser sentence than that

[379] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 40
[380] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 41
[381] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 42
[382] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 42
[383] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 43
[384] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 43

which followed from the bracket associated with the crime dependant on jurisdiction.[385] The Court thus concluded that "the relevant legal provision failed to satisfy the foreseeability requirement and provide effective safeguards against arbitrary punishment as provided in Article 7."[386]

In this case, the statutory law clearly defined the two alternative penalty brackets, but it failed to provide a procedural safeguard against arbitrariness. The prosecutor's discretion was not directed by guidelines nor was it subject to review by the courts. The prosecutor could thus independently and free from judicial review, define which offenses were serious and which were less serious. The Court seemingly did not find that case law had clarified which types of offenses would be pursued before which court. Arguably, even if such clarification had taken place, it would not have been the result of the courts' practice, but the prosecution's practice, which rested on indeterminable criteria and free from review even if it derogated from its own practice. There would be room left for arbitrariness, which could not be resolved by courts in practice, because the courts were in fact bound by the prosecutor's decision and had no recourse to address any concerns with the exercise of discretion. The prosecutor could freely choose to pursue two cases involving the same type of offense of the same degree of severity before a different court. In essence, the law provided sufficient guidelines to those enforcing the law, namely the prosecution. Arguably, this case shows that the Court considers that foreseeability and risk of arbitrary enforcement are not two distinct and separable concepts, but rather two concepts that go hand in hand. The difference between this case of unforeseeability and the other cases discussed in this section is that uncertainty in the form of vagueness in statutory language or other regulation may be gradually clarified by the courts. Uncertainty in terms of unreviewable discretion to choose between two clear and precise definitions of penalty brackets provided in law cannot, by definition, be clarified by the courts, who in this particular case, have no power to set the exercise of discretion aside even in the most suspect of circumstances. Vagueness in law can be cured by the courts, e.g. through strict construction, development of doctrines etc., whereas uncertainty in the exercise of unreviewable prosecutorial discretion cannot be resolved. Arguably, it would have been less controversial had the courts, rather than the prosecution, been granted the discretion to distinguish between less serious and more serious offenses and choose the appropriate penalty bracket based on its evaluation of the facts in each case.

---

[385] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 43
[386] *Camilleri v. Malta*, Judgment of 22 January 2013, para. 44

Article 7 is, arguably, primarily focused on the state's enforcement of the law against the individual applicant before the Court – as opposed to the hypothetical enforcement against others – and thus the Court will focus on whether the criminality of the applicant's conduct and the associated punishment for said conduct was reasonably foreseeable, the legal basis for conviction and punishment was existent and accessible. That is, the Court will evaluate whether the specific applicant's conviction and the imposed punishment was in conformity with article 7 of the Convention. Was the crime defined in law at the time of the conduct? Was the punishment for said crime defined in law at the time of the conduct? Could the applicant thus have foreseen the consequences of his actions?

Camilleri v. Malta arguably indicates that there are cases where the law itself is not in conformity with the Convention, because the law's uncertainty can never be cured since the law itself authorizes arbitrary enforcement in all cases – whether the power is actually abused or not. That is, there is an absence of safeguards against arbitrary enforcement inherent in the law in question that cannot be remedied through case law. The law is thus itself irreparably inconsistent with article 7, because it does not lend itself to a Convention-consistent construction, i.e. a construction that eliminates the unacceptably high risk of arbitrary enforcement. Such arbitrariness will continue to exist regardless of whether the outcome in the specific case before the court was seemingly justifiable.[387]

The applicant in Camilleri v. Malta was found in possession of 953 pills of ecstasy with intent to supply, which probably would amount to a serious offense in most jurisdictions. The fact that he was tried before a court where the more serious penalty bracket applied, which by the standard of other jurisdictions is arguably appropriate, it does not negate the unreviewable discretion of the prosecution under the national law, the prosecution's ability to bind the courts in terms of minimal penalty, and the resultant room that discretion leaves for arbitrary decisions. The safeguard against arbitrary enforcement was perennially absent, because the courts, even if faced with blatant abuse of power, would have no legal basis for handing down a lower sentence than the minimum sentence applicable due to the prosecution's choice of jurisdiction. The Government's attempt to convince the Court that the national courts in fact had a legal basis for imposing a sentence below the minimum in an article of the Criminal Code failed, because the language of said article explicitly excluded the possibility of its application to those convicted of the crime in question. The national courts had also confirmed that the article referenced by the Government was inapplicable in such cases. The Government could not provide any examples of decisions where the courts had applied the article to impose a lower sentence than the minimum. The Government could thus not provide any proof of safeguards against arbitrary enforcement. The Court

387

never addressed whether the prosecution's jurisdiction decision in the applicant's case had in fact been arbitrary. Rather, it focused on the inherent inability to provide safeguards in any case, even if there were an abuse of power.

This can be tentatively compared to the application of the US void-for-vagueness doctrine; more specifically, the distinction between facial vagueness (unconstitutionality of the law itself – that is, it has no constitutional application), and "vague as applied" (the law has constitutional applications, but is unconstitutional as applied in the case at hand), discussed below in the section on nullum crimen sine lege in the United States. Because there was no reading of the rules in *Camilleri* that could have reduced the risk of arbitrary enforcement, it could arguably be said that the rules were facially incompatible with article 7 ECHR; i.e. only the legislature, by way of a "do-over", could provide sufficient protection against arbitrary enforcement.

A case against Georgia revolved around an interesting question; whether the use of colloquial language, rather than conventional legislative language, rendered the language too unclear and thus failed to meet the qualitative requirements that follow from article 7 ECHR. In *Ashlarba v. Georgia*, the applicant had been convicted of the offense of being a member of the "thieves' underworld" and was sentenced to seven years' imprisonment. Interestingly, in its renewed fight against organized crime, the state had described the crime using colloquial language such as "thief in law", "thieves' underworld", "settlement of disputes using the authority of a thief in law", etc. The provision on being a member of the "thieves' underworld" was enacted along with additional legislation on organized crime and racketeering, in which the colloquial concepts of "thief in law", "thieves' underworld", among others, were explained. A "thief in law" is a criminal boss, who is considered to be the guardian of the "Thieves' Code". One of the most important tasks of a "thief in law" is to administer the "kitty" (the common monetary fund of the criminal underworld). Furthermore, a "thief in law" would give order to criminals of lower ranks, but would rarely engage in the criminal conduct themselves. Members of the "thieves' underworld" would recognize the rules organizing the "thieves' underworld" and actively pursue the goals of the underworld. Several socio-legal studies had shown that the informal authority of "thieves in law" pervaded into ordinary public life. These criminal bosses thus exerted social influence beyond their criminal underworld. Their rules of conduct were strictly enforced and failure to comply could result in punishment, including death.

The applicant's complaint centered on the imprecise language used in the criminal code; that being terms like being a member of the "thieves' underworld", and whether the meaning of the offense

was clear and foreseeable enough to regulate one's conduct accordingly.[388] The Court specifically noted the rationale behind the legislation; that being fighting organized crime more effectively.[389]

The Court referenced the socio-legal research that had been presented to it, when observing that "this criminal phenomenon was already so deeply rooted in society, and the societal authority of "thieves in law" was so high, that among ordinary members of the public criminal concepts such as "thieves' underworld", "a thief in law", "settlement of disputes using the authority of a thief in law", "*obshyak*" [kitty; the thieves' underworld's common monetary fund], and so on, were matters of common knowledge and widely understood."[390] (citations omitted) The Court thus considered that the national legislature had "merely criminalised concepts and actions relating to a criminal ("thieves") subculture, the exact meaning of which were already well known to the public at large."[391] The usage of colloquial language in the definition of the criminal offense, although interesting to the Court, was apparently rooted in the desire to ensure that the offense was easily understood by the public.[392]

The applicant, who was complaining that the definition of the crime of being a member of the "thieves' underworld" did not provide sufficient foreseeability, had during the investigation, explained that he knew that the person he was receiving instructions from had the title of "thief in law", as well as showing his knowledge of the underworld when visiting a potential future "thief in law" in prison, and he had also adjudicated in private disputes at the request of a "thief in law". It follows that the colloquial terms used in the legislation were not as entirely foreign to the applicant as he claimed.[393]

The Court continued, adding that, most importantly, the provision in question was a part of a larger legislative package on organized crime, and that a section in the law on organized crime and racketeering, which was a part of that package, comprehensively defined the already colloquial terms.[394] "Accordingly, the Court concludes that, after the criminalisation […] of the offence of being a member of the "thieves' underworld", the applicant, if not through common knowledge based on the progressive spread over decades of the subculture of the "thieves' underworld" over

[388] *Ashlarba v. Georgia*, Judgment of 15 July 2014, para. 35
[389] *Ashlarba v. Georgia*, Judgment of 15 July 2014, para. 36
[390] *Ashlarba v. Georgia*, Judgment of 15 July 2014, para. 37
[391] *Ashlarba v. Georgia*, Judgment of 15 July 2014, para. 38
[392] *Ashlarba v. Georgia*, Judgment of 15 July 2014, para. 38
[393] *Ashlarba v. Georgia*, Judgment 15 July 2014, para. 38
[394] *Ashlarba v. Georgia*, Judgment 15 July 2014, para. 39

the public at large, then by reference to section 3 of the Law on Organised Crime and Racketeering and, if need be, with the assistance of appropriate legal advice, could easily have foreseen which of his actions would have attracted criminal responsibility […].”[395] (citations omitted)

It is not clear whether the criminal code provisions would have passed article 7 muster on their own merit, absent the further clarification of the colloquial terms in another statute, seeing as the Court writes “most importantly” when it brings up the definition of the terms in another statute, which was a part of the same package. Usage of idioms, slang and the likes in legislation is, generally, hardly good draftsmanship – especially in the context of criminal law, where a higher standard of certainty is required. In *Ashlarba*, however, the terms’ colloquial nature appeared well-documented, and seen in the context of the legislative package and the comprehensive definition of the colloquial terms in another statute, the standard of guilt was sufficiently clear and foreseeable.

5.1.1.4 Foreseeability of facts

Some criminal provisions also implicitly require foreseeability as to fact. An excellent example is criminal trespass. Since intent is generally required, a defendant must have intended to trespass onto a property to which access was prohibited. In other words, the defendant must be able to foresee/know *where* the prohibited area is and that access is prohibited, for him to plan his conduct accordingly; a criminal trespass provision cannot serve any preventative purpose unless a person can know *where* not to go. Foreseeability of facts seems to be required under article 7, arguably, dependent on the subject matter of the criminal provision.

In *Custers, Deveaux and Turk v. Denmark,* the Court briefly addressed whether the applicants had notice of facts relevant to the application of the criminal provision prohibiting trespass. In 2001, the applicants were involved in a Greenpeace action to draw international attention to the use of the Thule Air Base’s radar for the the U.S. missile defense program and to collect information on the environmental impact of the presence of the Thule Air Base, located on the Dundas peninsula in Greenland.[396] Access by civilians to the area required permission from the Danish Ministry of Foreign Affairs and the U.S. authorities. The applicants, three Greenpeace protesters, were charged with and convicted of trespassing on the defense area. However, the exact size of the defense area

[395] *Ashlarba v. Georgia*, Judgment 15 July 2014, para. 40
[396] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 9

was disputed between the parties.[397] The applicants argued that the exact size of the defense area was confidential and therefore unknown to the public.[398] The airfield was shown on an official map of the area, however, there was no indication of the presence of an air base.[399] The applicants had only been in possession of a reproduction of that map. Only on a map published as an annex to a report on the relocation of the Thule Tribe in 1953 were there lines drawn on the map, a report and map which the Government used to argue showed a demarcation of the area of the air base.[400] The air base was not fenced off, and signs of "no entry" were only placed by the harbor and on the road leading between the airfield and another part of the base. Under the national law, an area need not be fenced off or display signs prohibiting entry in order for an unauthorized entry to constitute trespass. The applicants did not dispute this interpretation, but pointed out that the limits of an area must still be defined in some manner.[401] The Court stated that it was a crucial issue "whether the applicants could have foreseen that the area they had entered was "not freely accessible"."[402] Regarding the applicants access to a definition of the defense area the Court noted that there was no indication of an air base on official maps – only on a map annexed to a report from 1994 on the relocation of the Thule Tribe indicated some lines drawn, the origin and reason of which were ostensibly unclear. The applicants could therefore "not have been expected to obtain this map in preference to or in addition to the official map of the area they already possessed."[403]

The Court found no violation of article 7, because other circumstances showed that the applicants had clear intention to enter the defense area, and through their updates on the Greenpeace website had indicated they were aware they were inside the defense area.[404]

5.1.2 A "thin ice" principle?

Ashworth briefly brings up a so-called thin ice principle in his book Principles of Criminal Law as he cites Lord Morris' words that "those who skate on thin ice can hardly expect to find a sign which

[397] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 14
[398] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 14
[399] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 15
[400] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 15
[401] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 72
[402] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 90
[403] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 93
[404] See *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 95.

will denote the precise spot where he [sic] will fall in".[405] Ashworth argues that the principle ought not trump article 7, but notes that the ECtHR seems to leave room for the principle to effect the outcome of cases.[406] In both *Custers, Deveaux and Turk v. Denmark* and *Cantoni v. France*,[407] the Court noted that the applicants' could not have been unaware of the "risk of prosecution".[408] The concept of a thin ice principle has to do with situations where criminal defendants were aware or should have been aware of the risk of prosecution – that is, defendants, who ostensibly knowingly venture into a legal grey area and their conduct is on the fringe of illegal conduct.[409] In *Cantoni*, the Court stated that the foreseeability requirement may still be satisfied even if the person in question has to seek legal advice. The Court added in that respect that "[t]his is particularly true in relation to persons carrying on a professional activity, who are used to having to proceed with a high degree of caution when pursuing their occupation. They can on this account be expected to take special care in assessing the risks that such activity entails."[410]

In *Custers, Deveaux and Turk*, the Court noted that the absence of case law that could have contributed to foreseeability of the application of the executive order's penalty, "it was predictable that the applicants risked being sentenced to a fine if they entered the defence area without a permission."[411]

Ashworth challenges the legitimacy of the "thin ice" principle in light of article 7's absolute nature,[412] but *C.R. v. United Kingdom*, if anything, indicates that article 7 is not as absolute in practice. In *Cantoni*, the Court relies on the fact that the domestic appellate court had never upheld a decision that excluded a product from the scope of the provision and had always upheld decisions that included a product in the scope. In *Custers & Others*, other factors relevant to the case indicated the applicants were fully aware that they were trespassing. In *Cantoni* and *Custers & Others*, the Court may be hinting that the applicants were aware that their conduct fell within the

---

[405] Andrew Ashworth and Jeremy Horder: Principles of Criminal Law (2013), p. 62
[406] The same is suggested by Cian Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 9. Available at http://ssrn.com/abstract=1513623.
[407] As well as *Coeme & Others v. Belgium*, Judgment of 22 June 2000, para. 150.
[408] The Court also did so in *Liivik v. Estonia* when it found that there had indeed been a breach of article 7. The Court said: "The Court is not satisfied that the applicant could reasonably have foreseen that he risked being charged with and convicted of causing significant moral damage to the interests of the State for his conduct." (See para. 100)
[409] Andrew Ashworth & Jeremy Horder: Principles of Criminal Law (2013), p. 62
[410] *Cantoni v. France*, Judgment of 11 November 1996, para. 35
[411] *Custers, Deveaux and Turk v. Denmark*, Judgment of 3 May 2007, para. 81. See also *Coëme and others v. Belgium*, Judgment of 22 June 2000, para. 150 ("[…]the applicants, who could not have been unaware that the conduct they were accused of might make them liable to prosecution, […]")
[412] Andrew Ashworth & Jeremy Horder: Principles of Criminal Law (2013), p. 62

scope of the respective provisions, and thus were using the vagueness of the law as a defense in bad faith, so to speak. This is, however, purely speculation. The fact remains, though, that the Court's risk-related statements, could also be construed to mean that the protection under article 7 is not as absolute as it appears, in that the defendant seems to be inappropriately absorbing the consequences deriving unclear legislation, even though clarity of legislation is clearly the responsibility of the legislature. A thin-ice principle would then likely produce a chilling effect, since citizens would be avoiding conduct that is not clearly criminalized.

Furthermore, if the only thing that is foreseeable is that the statute enables or encourages arbitrary enforcement or unforeseeable enforcement; that which is foreseeable is merely the ever-looming possibility of prosecution for any and all conduct related to e.g. computers, then there is equally little protection from arbitrary use of power as if there had been no pre-existing law. A thin ice principle is thus a rather unsettling idea, because even a statute prohibiting "any conduct that offends the state in any way" technically provides foreseeability in the sense that one must always tread carefully with respect to the state, the thin ice principle neglects even the most serious risks of arbitrary enforcement, placing the risk of prosecution on the basis of an unclear statute with a defendant. Furthermore, the principles seems to invite the notion that if there is uncertainty about the criminality of the defendant's conduct there ought to be a presumption of criminality, rather than requiring the legislature to speak in a more concise manner. In other words, the principle also seemingly invites the possibility of extensive construction and analogy (because the thin ice looms in the penumbra and with analogous behavior), both of which are ostensibly precluded by article 7 ECHR.

As shown above, the ECtHR's case law leaves the distinct impression that article 7 ECHR is not necessarily a guarantee against unforeseeable extensive applications of criminal law (or judge-made retroactive criminalization) as long as the criminalization of the conduct is likely to be imminent (for that reason criminality is arguably foreseeable), the conduct is sufficiently morally reprehensible,[413] or the courts have never excluded anything from the scope.[414]

If the thin ice principle in fact does have a bearing on the outcome of article 7 ECHR complaints, then, arguably, one could argue that the legal basis for analogous application of criminal law provided by the Danish criminal code § 1 is not contrary to article 7 ECHR, since an extensive

[413] See discussion of *C.R. v. United Kingdom* above.
[414] See *Cantoni* above.

interpretation to cover conduct that is completely analogous to the prohibited conduct, yet not technically covered by the statute, could always be argued to be covered under a thin ice principle; thus, discouraging citizens from engaging in conduct that is analogous to conduct prohibited by statute. Furthermore, if it is indeed a thin-ice principle affecting outcomes of article 7 complaints, it would make it very difficult for applicants to succeed on an article 7 complaint, even where they may have been genuinely blind-sided by an unclear law, even objectively so, merely because that they should have recognized the lack of clarity of the statute as a significant risk factor.

5.1.3 Limitations of Article 7

5.1.3.1 Overbreadth vs. vagueness?

An important limitation on the reach of article 7 can be argued for. The limitation relates to the paper-thin line, or partial overlap, between overbreadth and vagueness. This differentiation has been explicitly made by commentators on US constitutional law in terms of challenges under the void-for-vagueness doctrine and the First Amendment overbreadth doctrine. The differentiation is discussed below in the section on US law.

The distinction between overbreadth and vagueness concerns becomes apparent in the ECtHR's case law at least in one aspect, namely, that criminal law policy is a matter for the states to decide.[415] The ECtHR does not, and arguably cannot, review the subject matter of a criminal provision (i.e. policy decisions), however objectionable the content, as long as the subject matter does not constitute an interference with the other substantive rights guaranteed by the Convention, such as freedom of expression, freedom of religion, freedom of association, etc.[416] Furthermore, article 7 is not applicable to procedural criminal law, including rules of appeal, law of evidence and statutes of limitation.[417]

[415] *H.M.A. v. Spain*, Application no. 25399/94, Decision of 9 April 1996 on the admissibility of the application, p. 117, and *Achour v. France*, Judgment of 29 March 2006, para. 44). See also Trine Baumbach: Strafferet og menneskeret (2014), p. 186
[416] See also Trine Baumbach: Strafferet og menneskeret (2014), p. 128-129
[417] Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 573

5.1.3.2 Protected conduct

In its decision on admissibility in the case *H.M.A. v. Spain*[418], the Commission stated with regard to article 7 (1), that "*[t]he Convention leaves the States free to designate as a criminal offence an act or omission not constituting the normal exercise of one of the rights that it protects and, consequently, to define the constituent elements of such an offence.*"[419] Thus, it is unmistakably clear that article 7 does not prevent overbreadth of criminal statutes (i.e. that the scope of a criminal provision reaches further than needed to cover the undesirable conduct, thereby covering innocuous conduct) as long as the provisions do not interfere with Convention-protected conduct. Such a limitation can also be inferred from the existence of positive rights, meaning rights, the existence of which are positively expressed in law, rather than conduct that is legal because it has not been made illegal (i.e. inferring legality from the lack of criminalization). Positive rights consequently place a limit on the legislature's power to decide criminal policy, whereas article 7 does not scrutinize criminal policy at all, and hence, does not oppose continuous reduction of individual freedom/autonomy; only if the particular legislative act, taking into account case law, fails to provide notice of the reduction in individual autonomy or clearly allows arbitrary enforcement. That is, article 7 provides no legal basis to scrutinize the existence or extent of criminalization, because it offers no "opposing force" to the state's right to form its criminal policy – only positive rights do. It only demands clear communication as to "what" and "when"; that is, what the rule prohibits, which in turn informs when the rule is triggered – "if, then". Article 7 is concerned with the quality of the communication (i.e. the law), not the content of the communication.

As noted above, the first prong of the test under articles 8 through 11 serves to determine whether an interference was "prescribed by law". The prong is largely the same as the test under article 7 as to whether a crime and its punishment has been defined by "law". Second, the interference must pursue a legitimate aim. Third, the interference must be necessary in a democratic society (pressing social need). The last prong calls for a proportionality test, where only the least intrusive interference needed is acceptable.[420] The addition of the last two prongs under the test carried out regarding interferences with rights makes it clear that the Court has authorization to scrutinize the breadth of national law. Thus, over-criminalization is "allowed" under article 7 as long as the legal

[418] Application no. 25399/94
[419] *H.M.A. v. Spain*, Application no. 25399/94, Decision of 9 April 1996 on the admissibility of the application, p. 117. Similar statement was made by the Court in *Kafkaris*, para. 151.
[420] Jacobs, White, & Ovey: The European Convention on Human Rights (2010), p. 311

consequences of an act or omission are reasonably foreseeable. Conversely, criminalization beyond what is necessary to pursue an otherwise legitimate aim will in all likelihood fail the additional tests used by the Court in connection with e.g. article 8-11 rights that positively place a limit on criminal policy decisions. It can arguably be derived from *Kokkinakis* that a law, albeit vague and overbroad on its face, can be consistent with the Convention when clarified through case law, as long as it is interpreted narrowly to not encroach unnecessarily upon the individual's positive rights.

Article 7 applies to all criminal legislation, not just that which infringes upon protected conduct. Article 7 will thus logically be a weaker protection, because there is less power to scrutinize national law. Because articles 8 through 11, trigger additional tests, such as that of whether the legislation in question pursues a legitimate aim and whether the interference with protected conduct is necessary in a democratic society, it is in some sense not odd that the Court supposedly prefers[421] to find violations under other articles over finding violations of article 7; however, this could also be explained from a lex specialis point of view. The Court's competence to review is broader under other articles in terms of national criminal policy. Rules that reach both non-protected conduct and protected conduct implies that the rule must be construed strictly.[422] Criminalization of assault for example is not an exception from a hypothetical opposing right to cause bodily harm to people. In fact, it requires an exception (excuse, defense, justification) in law for such conduct *not* to incur criminal liability. Free speech is a right positively provided for and free speech is the main rule rather than the exception under the Convention; thus, criminal law may, if there are justifiable reasons, as an exception, interfere with free speech, but only if necessary.

Although article 7 requires that criminal provisions not be interpreted extensively, e.g. by analogy, that is not to say that the opposite is true, i.e. that there is an obligation to construe criminal provisions strictly.[423] In this sense, it is helpful to distinguish between, on the one hand, purposely vague criminal provisions (act of the legislature casting a wide net in furtherance of its criminal policy) and, on the other hand, extensive interpretation of a reasonably clear provision so that it

[421] Cion C. Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 16

[422] *Başkaya and Okçuoğlu v. Turkey*, Judgment of 8 July 1999, para. 61 (addressing article 10 exceptions)

[423] The applicants in *Eurofinacom v. France* claimed a duty of strict construction of criminal statutes (*Eurofinacom v. France*, Application no. 58753/00, Decision of 7 September 2004), however the Court did not address this specifically. Furthermore, in the first decision in *Achour v. France*, the Court itself cited a rule of strict construction of criminal statutes (*Achour v. France*, Judgment of 10 November 2004, para. 37), but in the Grand Chamber's reversal (*Achour v. France*, Judgment of 29 March 2006) of the finding of violation of article 7, there is no mention of a rule of strict construction. Rather, the Court reverts to its normal boilerplate paragraphs on foreseeability.

"grows" beyond its language to encompass conduct that falls outside the natural meaning of the language (judicial expansion/creation of criminalization). Article 7 will prevent the latter, arguably only to some extent, but not necessarily the former. As shown above, gradual clarification of vague provisions through case law is not prohibited, insofar as the resultant development is consistent with the essence of the offense and could reasonably be foreseen. Essentially, it is the difference between the courts, metaphorically, coloring inside the lines and the courts coloring outside the lines, where the lines represents the limits of the language's ordinary meaning and the goal is to keep the resultant picture neat and tidy.

However, in one aspect article 7's protection may exceed that of articles 8 through 11. The critical time relevant to the article 7 examination of whether a crime was defined in law is the time the conduct took place. The relevant time for whether an articles 8-11 interference was prescribed by law is the time of the interference – not the time of the conduct, unless the interference leads to criminal prosecution (which would then trigger article 7). Therefore, article 7 allows for no retrospective criminalization, whereas interferences with article 8 through 11 rights can be retrospective.[424]

5.1.4 Nullum crimen, nulla poena sine lege in EU law

The principle of no crime, no punishment without law is a general principle in EU law and enshrined in article 49(1) of the Charter of Fundamental Rights of the European Union. Article 49(1) states:

> "No one shall be held guilty of any criminal offence on account of any act or omission which did not constitute a criminal offence under national law or international law at the time when it was committed. Nor shall a heavier penalty be imposed than the one that was applicable at the time the criminal offence was committed. If, subsequent to the commission of a criminal offence, the law provides for a lighter penalty, that penalty shall be applicable."[425]

[424] See e.g. *Başkaya and Okçuoğlu v. Turkey* where the Court found that the interference was not prescribed by law because the interference took place after the relevant law was repealed. However, the crime was defined in law in terms of article 7, because at the time of the conduct, the relevant law was still in force. See also Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 8

[425] The ECtHR has interpreted article 7 to include a duty to apply a later provision if the punishment under the newer provision is more lenient than the older. Such a duty does not follow from the language of article 7 ECHR. Jon Fridrik

Article 52(3) of the Charter states that where rights in the Charter correspond with the ECHR the right has the same meaning and scope as the latter.[426] Article 49(1) thus has the same meaning and scope of article 7 ECHR.

Article 7 ECHR embodies the principle that only the law can define crime and punishment. However, EU law cannot create or aggravate criminal liability in and of itself, independently of implementation of the EU rules in national law.[427] A legal basis must thus exist in national law at the time of the conduct, since EU law cannot independently create or aggravate criminal liability. Similarly, national law cannot be interpreted extensively with reference to EU law (e.g. as a response to having failed to implement EU rules) – that is, principle of conforming interpretation – thereby extending the scope to conduct, which would not otherwise be covered by the language of the domestic provision, to the detriment of the defendant. If the EU legislation has been implemented incorrectly or has not been implemented (whether the time for implementation has elapsed or not), the legal basis requirement for description of crimes in national law places a limit on the member state's ability to interpret and apply national law in light of the EU legislation. Such a failure to implement criminal provisions cannot be retrospectively corrected by the member state through interpretation and construction in national law in order to comply with EU law, as such a "correction" would amount to retrospective criminalization. The duty of conforming interpretation cannot override the principles of nullum crimen, nulla poena sine lege.[428]

Furthermore, it bears mentioning that if national legislation is an implementation of EU law, even if it is copied almost, or entirely, verbatim into national law, the member state can still be held responsible if the legislation violates article 7 ECHR.[429]

Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010), p. 573, citing Scoppola v. Italy of 17 September 2009, para. 103-109

[426] Article 52(3): "In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection."

[427] C-105/03 Pupino, pr. 45 (the case involved a framework decision and procedural rules) and C-80/86 Kolpinghuis Nijmegen, pr. 14 (the case involved a directive that had not been implemented in national law at the time of the conduct)

[428] Joined cases C-74/95 and C-129/95 X

[429] *Cantoni v. France,* Judgment of 11 November 1996, para. 30 ("The fact, pointed to by the Government, that Article L. 511 of the Public Health Code is based almost word for word on Community Directive 65/65 (see paragraph 12 above) does not remove it from the ambit of Article 7 of the Convention (art. 7).")

5.1.5 Summary

Article 7 seemingly protects against arbitrary enforcement of a criminal law that either does not exist or is so vague that it provides no standard of guilt thus depriving the citizen of the ability to plan his conduct. Such enforcement of criminal law is not only unforeseeable to the regulated, but may also be arbitrary in nature.

In terms of protected conduct, criminal rules impacting such conduct create exceptions from the main rule that such conduct is legal; but only if the criminalization follows legitimate aims and is necessary in a democratic society. Such criminal rules must be strictly construed in order to support effective, rather than illusory, rights. Therefore, the Court must, in some instances where the rule follows a legitimate aim, also make sure the rule is applied only where there is a socially pressing need.

Neither article 7 nor articles 8 through 11 prevent the adoption of vague rules that need to be clarified gradually through case law. The question of legality hinges on whether the result of such development is consistent with the essence of the crime and could reasonably be foreseen. However, vague rules may also create a chilling effect on the exercise of positive rights, if the beneficiaries of these rights risk prosecution. A similar chilling effect arises under rules that regulate non-protected conduct, if a thin-ice principle places the burden of unclear legislation on the defendants whose conduct was not definitively within the scope of the criminal provision. Only the legislature can provide clear description of prohibited conduct. A thin-ice principle would further narrow the protection under article 7, because such a principle demands little else than that the lack of foreseeability is foreseeable, creating a presumption of criminality within a possibly very large penumbra, and perhaps even outside the penumbra. This is hardly in accordance with a requirement that criminal rules must be clear.

The degree of required foreseeability depends on the subject matter, the area of law, and the characteristics and number of the regulated. Business regulation is for example subject to a less stringent foreseeability requirement. Furthermore, foreseeability of fact relevant to the provision in question may be required, e.g. maps demarcating an area that is not freely accessible in connection with applying a trespass provision.

Overall, it is unclear to which extent extensive interpretation is prohibited under article 7, especially in light of *C.R. v. United Kingdom* and *Cantoni*. Maybe it is a case of "you know it when you see it" (see below about void-for-vagueness in US law). If the slate is blank, that is, the case is not a reversal of prior case law, but clarification within the scope of the provision, judicial development seems to be fine. If the vagueness cannot be cured through case law, the provision is likely to fail an article 7 test – especially so, when the courts have adopted a vague standard in their interpretation of an already vague language.[430] If, however, the case at hand involves a departure from prior case law, the rule will likely fail an article 7 test, ostensibly unless the Court finds moral reasons to decline to find a violation. All article 7 applicants are bound to have been convicted of a crime, which arguably makes them far less sympathetic[431] than articles 8-11 applicants; however, article 7, arguably as opposed to articles 8-11, is not about condoning the actions of the applicant, but about demanding that the state give the regulated (including the applicant) sufficient notice in law of the illegality of the conduct prior to the applicant engaging in that conduct.[432]

5.2 Nullum crimen sine lege in Denmark

5.2.1 The Danish Criminal Code § 1

In Danish law, only the law can define a crime and its associated punishment. Although this also follows from Denmark's international obligations under article 7 ECHR, the principle of legality in Danish criminal law dates back to 1866 when the first comprehensive criminal code was passed into law.[433] Prior to 1866, Danish criminal law was marked by judicial creation of crimes, because Christian V's Danish Law (*Christian den 5tes Danske lov)* of 1683 and a number of subsequently issued regulations defined only a very limited number of crimes, and those crimes were formulated in casuistic terms.[434] The judges of the time therefore almost immediately found themselves in a position where they had to decide cases involving unacceptable, yet not criminalized, behavior that

[430] See *Camilleri* and *Liivik*.
[431] See also Cian C. Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 16. Available at http://ssrn.com/abstract=1513623.
[432] Even if the marital immunity in *C.R. v. United Kingdom* were (and it may have been) a violation of the UK's positive obligations under the ECHR, it is not the role of the ECtHR to help the UK retroactively remedy that violation by allowing another.
[433] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 140
[434] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), pp. 140-141

did not fit the few and casuistically worded statutory definitions provided for in the 1683 law.[435] At the time, Denmark was an absolute monarchy, and it was not until the Constitution of 1849 that the judicial and legislative powers were separated.[436] For that reason, prior to 1849, the Danish Supreme Court was presumed to be acting on behalf of the monarch, who was the highest judicial authority, when the Court "supplemented" the statutes by declaring conduct criminal because it was malum in se, its contradiction with the spirit of the law and its principles, etc.[437] The court would then impose an arbitrary sentence for the crime.[438] The constitutional separation of the legislative and judicial powers in 1849 was critical in paving the way for the principle of legality in criminal law adopted as part of the 1866 criminal code.[439]

The principle of legality protects the citizens against the state's arbitrary use of power.[440] Legality demands that only the legislature, in exercising its legislative power as representatives of the people and following the legislative procedure, can define acts and omissions as crimes and define the associated punishment.[441] Because crimes are defined by the legislature, the courts, being entrusted with applying the laws to resolve conflicts, are in turn bound by the legislature's directives in those laws. The directives, that is, the statutory texts, are rarely so clear that they never require the courts to clarify them by way of interpretation and construction.[442]

The principle of legality, finding its expression in the criminal code's § 1, has remained largely unchanged since the 1930 overhaul of the 1866 criminal code.[443] Its translation reads:

> "Only acts punishable under a statute or entirely comparable acts shall be punished. […]"[444]

The Danish Criminal Code § 1 is an expression of the principles nullum crimen, nulla poena sine lege and states that punishment can only be imposed for conduct which is criminalized by law or for conduct that is the complete analogous to the criminalized conduct. According to the criminal code's § 2, the principle applies equally to conduct criminalized in special legislation. A legal basis

---

[435] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), pp. 141-142
[436] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 150
[437] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 89
[438] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 141
[439] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 150
[440] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 89
[441] See Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 89 and Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 155
[442] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), pp. 89-90
[443] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 140
[444] Translation from Lars Bo Langsted: Criminal Law in Denmark (2014), p. 85

must exist which 1) criminalizes the conduct, and 2) prescribes punishment for the conduct in question.[445] The strict legal basis requirement only applies where the resultant decision is to the defendant's detriment.[446]

5.2.2 "Statute"

In order to understand the extent of the protection provided under § 1, it is imperative to understand to what the word "statute" refers.[447] The concept of "statute" in § 1 should be understood as meaning that the legislature has taken action in accordance with the legislative process described in the Constitution.[448] Only the legislature has the authority define crime and prescribe punishment. Legislative power rests with the king and the parliament in unison, according to the Constitution's (*Grundloven*) § 3.[449]

However, it is not uncommon that penalty is attached to a violation of provisions in executive orders or ordinances adopted under a statute containing a provision delegating authority to make rules; that is, the legislature has delegated some of its authority to define crime and punishment. The executive order must have a legal basis in a statute, though. The legal basis for the executive order, i.e. the enabling statutory provision, defines the scope of the executive branch's authority to create rules within the area in question. Such executive orders can describe crimes and prescribe punishment as long as the enabling provision delegates such authority, and then only within the scope defined by the enabling provision. In cases involving violation of executive order provisions, the legality of the executive order and its reach should be evaluated in light of the enabling provision in the primary law. If the executive order has overstepped the boundaries of the authority granted in the enabling provision by criminalizing the conduct in question, there is no need to determine whether the criminal provision in the executive order has been violated, since the legal

[445] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 152
[446] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 90
[447] Note that the Danish language version of § 1 uses the word "lov", which could linguistically refer to both "law" and "statute". However, compared to the concept of "law" in article 7 ECHR (and in English, more generally), the Danish word "lov" has a much narrower meaning because "lov" in a Danish context would typically never encompass case law, but can be understood as encompassing rules adopted based on a (narrow) delegation of legislative power to the executive branch (typically the ministries).
[448] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 89 and Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 155
[449] It follows from the Constitution's § 22 and lack of practice that the King's legislative power is largely ceremonial, as his role is confined to signing the laws. The King's veto power has not been used since 1865 and is considered desuetude. Karnov commentary to the Constitution's § 22, note 58

basis for the criminalizing provision is absent.[450] The court must acquit.[451] The same applies in terms of ordinances enabled by a primary law.

Whether there is a legal basis for conviction and punishment for a crime, is determined by examining the text of the substantive provision.[452] The text limits the scope of the provision, but statutory language is rarely, if ever, so clear that it never requires interpretation. The scope is, thus, found through interpretation of the statutory language.[453] The act must fall within the scope of the provision's language. If it does not, there is no legal basis for conviction and punishment.

In Danish law, there is no constitutional rule or doctrine that imposes qualitative clarity requirements on the legislature when they adopt statutes in general or criminal statutes specifically. Such a clarity requirement does not follow directly from the language of the criminal code's § 1 either. Seeing as the principle of legality in § 1 was enacted to avoid arbitrary convictions and punishment by the courts by requiring a legal basis, it follows, at least indirectly, from its rationale, albeit not from its text, that for such a legality requirement to be effective, qualitative requirements such as foreseeability, clarity and precision are not irrelevant factors when deciding whether to apply a statute or not.

Even if a criminal provision, adopted by the legislature, is impossibly vague, the Danish courts are technically not competent to rule on the provision's validity on that basis.[454] The courts cannot avoid clarifying vague provisions where clarification is possible.[455] However, that is not to say that the courts are required to *convict* on the basis of very vague language.[456] The courts can, and should, decline to convict on the basis of a provision, if they find the provision so vague that it cannot reasonably be determined whether the conduct in question is covered by the provision; that is, the courts would find that there is no a legal basis for conviction and punishment.[457] The result will then be an acquittal, not due to the legislature's failure to meet a formal clarity requirement

[450] As examples, Waaben and Langsted cite e.g. U.1979.188V as an example where the criminalization in question exceeded the scope of the enabling statutory provision.
[451] Peter Germer: Statsforfatningsret (2007), p. 130
[452] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), pp. 172-173
[453] Alf Ross: Om ret og retfærdighed (2013), p. 159 (All statutory interpretation has its point of departure in a text.)
[454] See Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161
[455] See Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161
[456] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161, and Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 91
[457] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 91 and Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161

derived from higher-ranking rules, but because there is no clear legal basis to convict.[458] Thus, even a statute plagued with vagueness, which then might never be used because it cannot serve as a legal basis for a criminal conviction, is still a "statute" within the meaning of the criminal code's § 1. According to Baumbach, if the court declines to convict because it cannot determine whether the conduct matches the elements of the crime as it is described, the courts are basing their acquittal on the absence of a legal basis for conviction in the case at hand, and that should not be confused with application of a clarity principle.[459] Hence, although the courts cannot declare a statute void for vagueness on constitutional grounds, they can refuse to apply the statute, because the statute does not provide a clear legal basis to convict; this may then, impliedly, send a message to the legislature that it must speak clearer.

In my opinion, a determination of lack of legal basis can relate to two different situations, both involving uncertainty, but where only the first situation substantially implicates lack of clarity[460]. The first situation refers to cases where the doubt as to applicability relates to the linguistic scope of certain words in a provision, words which already have a determinable meaning. Take, for example, the question whether the word "ship" also extends to include a "rubber dinghy".[461] In this situation, the lack of clarity relates to whether a word can be construed so *widely* as to encompass objects that do not normally fall within the category of sea vessels definable as "ships". The second situation refers to cases where the uncertainty, relates to indeterminable standards, namely those that tend to be subjective in nature. That is, the uncertainty arises in the first situation because there is doubt as to whether the "core" of the provision suggests that "rubber dinghy" (in the penumbra) should fall inside or outside the scope. In the second situation, the "core" itself is ill-definable. The criminal conduct is ostensibly indeterminable, and the provision's language does not make it possible to distinguish between legal and illegal conduct. The court lacks guidance, and absent a meaningful method of distinguishing between the legal and the illegal, the decisions become characterized by arbitrariness. To summarize, the first situation encompasses cases where the word in question is sought to be *expanded* with respect to the natural meaning of the language – that is, clarification as to legal effects in the linguistic penumbra. The second situation encompasses cases where there is doubt as to what the "core" is, and even more so, doubt as to whether a penumbra even exists if the core from which it flows does not exist. An example could be a provision that prohibits a person from conducting themselves in a way that is annoying – a standard which is entirely subjective.[462] In comparison, "ship" is capable of objective, gradual clarification in the provision's penumbra even though it might be disputed initially how large a sea vessel must be to qualify as such.

---

[458] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161, and Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 91
[459] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 161
[460] "Clarity" as a reference to linguistic clarity.
[461] Example is derived from a Danish case concerning "ships" and "rubber dinghies". U 1999.2074V.
[462] The meaning of "annoying" was at the center of *Coates v. City of Cincinnati*, 402 U.S. 611 (1971). The word "annoying" was deemed to be too unclear a standard.

5.2.3 Clarity as "good draftsmanship"

There is no Danish legal requirement, constitutional or criminal-law, that mandates clarity in legislation. However, it is clear that vague laws make it hard, and at times impossible, for the regulated person to plan his conduct, or even for the courts to apply the law at all. The law would not have the preventative effect to which it aspires, if the regulated cannot determine what conduct the law aims to prevent. It is also clear that the task of ensuring clarity in the statutory language belongs to the legislature, since it is the legislature that adopts the laws.

The Danish Ministry of Justice published guidelines in 2005 on the quality of law (good draftsmanship[463]). The guidelines state that it is in the interest of the public, the Parliament, the media and those administrating the law, that the rules in the guidelines are respected.[464] The majority of legislation is aimed at the public in order to regulate conduct. Therefore, it serves the fundamental principle of legal certainty that the public, to the widest extent possible, is able to understand and hence plan their conduct in accordance with the law.[465] Those applying the law, e.g. lawyers, judges, prosecution authorities and other administrative authorities, also have an interest in good draftsmanship.[466] The guidelines explicitly state that the quality of the law cannot be compromised with, by relying on the legal professionals' training to resolve the interpretational problems that inevitably arise out of poor draftsmanship.[467] Furthermore, the Ministry emphasizes that drafting laws in good and clear language is a necessary precursor to a uniform application of the law, and thus also a necessary premise for foreseeability and legal certainty.[468] Living up to the ideal of clear and intelligible laws also promotes better media discussions, as well as enabling the members of Parliament to better and more quickly understand bills before debating them.[469]

According to the guidelines, the clarity requirement in terms of the law is primarily aimed at the statutory language. The guidelines emphasize that clarity is of even greater importance when the law in question acts as a legal basis for imposing restrictions on citizens, e.g. criminal punishment, confiscation, etc.[470] The added importance is due to an elevated need for foreseeability in such

[463] In Danish "god lovgivningsskik".
[464] Vejledning om lovkvalitet (2005), p.8
[465] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 8
[466] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 8
[467] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 8
[468] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 8
[469] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 8
[470] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 12

cases.[471] The Ministry does not provide any precise rules on how to compose drafts, but it does give examples of what constitutes good statutory language: Simple, concise and precise language, both as regards choice of words as well as style, short and clear sentences, consistency in use of words, only use words in their ordinary meaning as far as possible, and no use of foreign words or technical terms if that can be avoided[472]; the latter, particularly applies with regard to legislation that is aimed at the general public rather than a specific group of actors.[473] Moreover, ambiguous and superfluous words should be avoided.[474]

Article 7 ECHR is mentioned in the guidelines as a legislative restraint. The Ministry acknowledges that article 7 ECHR limits how vague and imprecise criminal law provisions can be, and emphasizes that it is critical that the drafters of the law are aware of the precision requirements when describing crimes.[475]

It is important to note that the Ministry's guidelines represent an expression of good draftsmanship as ideal. Just as article 7 ECHR does not require the impossible, the guidelines do not expect the impossible. Language is always capable of ambiguity to some extent. Rather than attempting to eliminate ambiguity altogether – an impossibility – it is a question of limiting ambiguity and vagueness to the greatest extent possible without rendering the law too rigid and unpractical to administrate.

Ultimately, the guidelines are just that – guidelines. Even if a defendant were facing a novel and creative application of a broadly/vaguely worded statute, the guidelines are not a source of legal recourse.

5.2.4 "Acts"

"Acts" (or "forhold" in Danish), in the criminal code's § 1, encompasses both acts and omissions, and "acts" should be read as meaning the "actus reus" of a substantive provision.[476] Thus, to

[471] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 12
[472] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 12
[473] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 13
[474] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 13
[475] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 36
[476] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 191

determine what constitutes an "act" in terms of the criminal code's § 1, each element of the substantive provision in question must be taken into consideration.[477]

It should be noted that the Criminal Code's § 1 does not technically require the substantive criminal provision include mens rea or that other fundamental concepts such as causation are described in law.[478]

5.2.5 Limitations of the legal basis requirement

Neither the Constitution nor the criminal code's § 1 prohibits intentional or unintentional over-criminalization (overbreadth), bad draftsmanship or vague language. The legislature is free to exercise its legislative power, including criminalizing any conduct as it sees fit.[479] The primary restraints on legislative power follow from the Constitution and constitutional principles, EU law (e.g. the four fundamental freedoms) and international obligations, such as the European Convention on Human Rights.[480]

There is no constitutional prohibition against retroactive criminalization or increase in penalty.[481] The criminal code § 1, according to its wording, only requires the existence of a legal basis at the time of adjudication – not prior to the conduct.[482] The criminal code § 3 also states that if the law that regulates the conduct has changed since the conduct took place, the newer law applies unless it carries with it more severe punishment.[483] As is the case with the criminal code § 1, § 3 is only a statutory provision that can be changed/overridden by newer law.[484] However, it is considered a fundamental legal principle, even though it is not a constitutionally derived one, that retrospective punishment or increase in punishment is not allowed.[485] Furthermore, as discussed above, even if no

[477] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 191
[478] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 153
[479] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 31
[480] Justitsministeriet: Vejledning om lovkvalitet (2005), p. 31. The ECHR has been incorporated into Danish law, and thus, is Danish law as opposed to many other conventions. See also the above chapter on sources of law.
[481] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 105. See also Peter Germer: Statsforfatningsret (2007), p. 143.
[482] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 153
[483] See Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014), pp. 35-36
[484] Peter Germer: Statsforfatningsret (2007), p. 143.
[485] Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2012), p. 105

such legal principle existed in Danish law, article 7 ECHR prohibits criminalization after the conduct took place but before adjudication.[486]

Analogous application of criminal law – i.e. application of provisions to conduct that falls outside the statutory language – is a close cousin of retroactive criminal legislation. The criminal code § 1 does not prevent analogous application of criminal provisions entirely; in fact, it permits it to a limited extent. An analogous application of a criminal provision does, however, require that the conduct in question is completely analogous to the conduct described in the provision. Thus, in practice, the scope for analogous application is rather narrow. By using an analogy one attempts to explain A by using B as a reference. B must be vastly similar (not necessarily identical[487]) to A in order for the analogy to make sense.[488] However, if the similarities, which lead to the analogy, are false assumptions, or if we know too little about the things we are comparing, the analogy is likely to be erroneous and it will not help us understand A at all.[489] Hence, analogies carry with them a degree of risk, even when an analogy, at face value, appears convincing.[490] In many instances, the analogy may not be relevant to the context. The human brain is sometimes described as a biochemical computer. Absent any context, the analogy appears quite convincing. But if the analogy is put into the context of computer crime, it inarguably makes no sense to try to apply a provision prohibiting unlawful interference with a computer to a case involving a defendant who has knocked a person unconscious. Clearly, it does not suffice that the analogy in and of itself is convincing, and the accuracy of the analogy and its relevance depends on the context.

In terms of the § 1, analogous application means application outside the scope of the provision's language, but only insofar as the conduct is wholly analogous to the prohibited conduct, and the same reasons for applying the law exist for both the conduct that falls inside the scope and the conduct in question that is outside the scope.[491] Hence, the reasons for criminalizing B, and the

[486] See also Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2011), p. 91. It follows from the ECtHR's interpretation of article 7 in *Scoppola* that if the punishment is more lenient under the new law, the newer law must be applied. The language of article 7 does not expressly provide for such a right.
[487] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 396
[488] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 395
[489] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 395
[490] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 395
[491] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 396

protective interests underlying criminalizing B, must also be valid for A. Moreover, there can be no legally relevant difference between A and B that favors the two being treated differently.[492]

An analogous application thus goes beyond even the broadest reading of the language,[493] because § 1 allows application of the substantive provision even though the conduct technically falls outside the language of that substantive provision.[494] Bear in mind though, that § 1 is not itself the legal basis for conviction, but a legal basis to extend the scope of the substantive provision which describes conduct that is wholly analogous to the defendant's conduct. As a further possible limitation on analogous applications: Although analogous application of a substantive provision does not require that the conduct in question is unregulated, i.e. that there is a lacuna in the law, an analogous application is presumably unjustified if the conduct is directly covered by another provision.[495]

The legal basis for analogous application of a substantive provision in § 1 is rarely used. One example of its usage was in a case[496] that involved a provision that enabled the court to issue an order prohibiting the public naming of the defendant. In the case, the court had issued such an order, but a newspaper article, instead of naming the defendant, described him in terms of his age, nationality, job title and place of employment, which effectively identified him to the public. The Supreme Court found that such information identified the defendant just as effectively as had the newspaper article used the defendant's name.[497] The prohibition of the publishing of other information than the defendant's name did not follow from the statutory text, even in its broadest reading, but it followed from the essence of the criminal conduct.[498]

Regardless of the fact that § 1 constitutes a legal basis for analogous application of criminal provisions to the detriment of the defendant, analogous application – that is, application outside the scope of the language – inherently means that the courts usurp legislative power to an extent when applying substantive criminal provisions analogously.[499] Furthermore, it is unclear whether every

[492] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 407-408 (quoting Alf Ross: Om ret og retfærdighed, p. 176)
[493] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 396
[494] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 396
[495] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 408-409 (citing Peter Blume: Juridisk metodelære, p. 160 et seq.)
[496] U 1988.365 H
[497] See discussion of case in Trine Baumbach: Det strafferetlige princip (2008), p. 414-415
[498] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 415
[499] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 396

shade of analogous application of criminal provisions allowed by § 1 would be consistent with article 7 ECHR, which has been interpreted to prohibit extensive interpretation of criminal provisions, including interpretation by analogy. As shown in the section on article 7 ECHR, the Court does not prohibit gradual clarification, but where the line is drawn between "gradual clarification" and "extensive interpretation" is uncertain. In light of the ECtHR's case law, it is tempting to conclude that the Court, if faced with a complaint about the Danish criminal code § 1, would likely state that the applicant (such as the newspaper from the example above) could not have been unaware of the risk that he might be prosecuted for the conduct; particularly given the rather limited extent of analogy allowed under § 1, and perhaps given a case where it is quite clear that the applicant skirted illegality by way of technicality despite having caused the exact harm the provision aimed to prevent.

5.2.6 Summary

Clarity and precision in criminal statutes in Denmark is not a requirement mandated by law, nor does it constitute a constitutional guarantee, due process right, or the likes. Clarity and precision are concepts that relate to the wording of a statute, i.e. the quality of the legislature's draftsmanship. However, lack of clarity and precision in describing the criminal conduct brings in its train reduced foreseeability as to the application of the statute. In other words, foreseeability can be said to be a function of clarity, precision, and consistency in interpretation and application. Only clarity and precision are directly within the legislature's control, although, there is arguably a relationship between good draftsmanship and the subsequent degree of consistency of judicial interpretation and application.

Clarity and precision alone cannot guarantee foreseeability, but since the statutory text constitutes directives to the courts (as well as notice to the citizens), the text acts as a constraint on the court minimizing the possibility of arbitrary and unforeseeable applications. The Danish Ministry of Justice has issued guidelines on good draftsmanship that express the need to draft provisions that are as clear and precise as can be with respect, mindful of the rigidity and complexity of too much precision, and the impossibility of achieving absolute certainty. Although no legally mandated clarity requirement exists in the Constitution or the criminal code, article 7 ECHR imposes qualitative requirements that at the very least rest on the presumption that statutory language must be clear enough for it to direct the courts when they clarify uncertainties as to the provision's

application. Should Danish courts apply a provision that is devoid of standards or apply it in such a way that its application was not reasonably foreseeable, the application would likely be in violation of article 7 ECHR.

Should the statutory text be entirely standardless, rather than finding a provision or statute unconstitutionally vague (which would be entirely unprecedented given the Danish courts' lack of competence to do so), Danish courts will acquit on the grounds that there is no legal basis for conviction, as required by the principle of legality in the criminal code's § 1.

Analogous application of criminal provisions is not entirely outlawed, seeing as § 1 provides a legal basis for doing so when the conduct in question is wholly analogous to the conduct described in statute. The courts use analogy with great restraint, making the cases involving analogy in a criminal context few in numbers. Article 7 ECHR may or may not place a limit on this already narrow access to analogous application. If a thin-ice principle is influencing the ECtHR, it is unlikely that any application of the Danish criminal code § 1, as long as done with restraint, constitutes a violation of article 7 ECHR. If there is no such principle, the possibility of an article 7 violation still looms.

5.3 Nullum crimen sine lege in the United States

As appears to be the case in US law, the principle nullum crimen sine lege is tenuously associated with the constitutional principles prohibiting retroactive law-making and vague criminal laws.[500] The prohibition against ex post facto laws is stated in clause 3 of article I, section 9 of the United States Constitution. This clause applies only to the legislature. The prohibition against vague criminal laws is often considered to follow from due process requirements under the Fifth Amendment[501].[502]

[500] Markus Dirk Dubber, Oxford Handbook of Comparative Law, p. 1313
[501] Fifth Amendment regarding federal laws, and Fourteenth Amendment regarding state laws.
[502] Wayne LaFave, Criminal Law, p. 109, and, Dubber, Oxford Handbook of Comparative Law, p. 1313

5.3.1 Legality

One of the basic premises of criminal law is that conduct must be criminalized prior to its commission so as to provide fair warning to the citizens. The principle of legality, or nullum crimen, nulla poena sine lege, "is reflected in the ex post facto prohibition, the rule of strict construction of criminal statutes, the void-for-vagueness doctrine, and the trend away from open-ended common law crimes."[503]

In the 1798 case, *Calder v. Bull*[504] the US Supreme Court gave a list of what it perceived to be ex post facto laws. First, "Every law that makes an action done before the passing of the law, and which was innocent when done, criminal; and punishes such action." Second, "Every law that aggravates a crime, or makes it greater than it was, when committed." Third, "Every law that changes the punishment, and inflicts a greater punishment, than the law annexed to the crime, when committed."[505] Fourth, "Every law that alters the legal rules of evidence, and receives less, or different testimony, than the law required at the time of the commission of the offense, in order to convict the offender."[506]

The first three examples provided by the Court concern substantive law, whilst the fourth concerns procedural law.[507] The most obvious cases of retroactive legislation concern the creation of new crime and applying the law to conduct predating the legislation, the elimination of elements of an offense, and elimination of defenses, which were available at the time of the conduct.[508] The Supreme Court has stated that the ex post facto prohibition serves to important purposes. First, "to assure that legislative acts give fair warning of their effect and permit individuals to rely on their

[503] Wayne LaFave, Criminal Law, p. 11 (citations omitted)
[504] 3 U.S. (3 Dall.) 386, 1 L.Ed. 648 (1798)
[505] The second and third examples are an expression of the same idea. Wayne R. LaFave: Criminal Law (2010), p. 115.
[506] See Wayne R. LaFave: Criminal Law (2010), p. 115 et seq.
[507] Wayne R. LaFave: Criminal Law (2010), p. 115
[508] Wayne R. LaFave: Criminal Law (2010), p. 116. Also, as opposed to article 7 ECHR (which does not apply to rules concerning execution of sentences), the Supreme Court has held that the ex post facto prohibition does apply to cases involving e.g. removal of early release credits, changes in rules on good time towards early release etc. See Wayne R. LaFave: Criminal Law (2010), p. 116-117. Cf. *Kafkaris v. Cyprus*, where the ECtHR reiterated that rules on execution of sentences do not fall within the scope of article 7 ECHR. Similarly to ECtHR rulings, the ex post facto prohibition does not prevent extensions of a statute of limitations for crimes the statute of limitations of which has not yet elapsed. See Wayne R. LaFave: Criminal Law (2010), p. 120.

meaning until explicitly changed".[509] Second, that it "also restricts governmental power by restraining arbitrary and potentially vindictive legislation."[510]

Clearly, these ex post facto prohibitions apply only to legislation and not case law, and generally only apply in criminal matters.[511] Inherently, case law is retrospectively operating judicial interpretation, and thus, the ex post facto prohibition is applied in a narrower version in that respect.[512] However, the purposes of the ex post facto prohibition are not well served if judicial decisions always have retroactive effect, since some applications of the law might lack fair warning or might be arbitrary in nature. For that reason, the Supreme Court has held that the due process clause prevents courts from doing what the legislature is prohibited from doing under the ex post facto clause.[513] That is, if the legislature cannot pass a law that criminalizes conduct that took place before the law's enactment, neither so can the courts construe the law so as to achieve the same result.[514]

The classic examples of prohibited ex post facto judicial decisions are the overruling of a precedent the application of which would have resulted in acquittal for the defendant, disallowing a defense permitted in earlier cases, and interpreting a statute as applying to conduct previously excluded from its scope.[515] It appears, though, that if a judicial construction of a statute is "unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue", an acquittal is appropriate in light of fair warning concerns.[516] In the case of a statute that on its face may be unconstitutionally vague or broad, the clarifying judicial construction that saves the statute from unconstitutionality, is applied retroactively, insofar as "the limiting construction is a relatively

---

[509] Wayne R. LaFave: Criminal Law (2010), p. 116 (citing *Weaver v. Graham*, 450 U.S. 24, 101 S.Ct. 960, 67 L.Ed.2d 17 (1981))
[510] Wayne R. LaFave: Criminal Law (2010), p. 116 (citing *Weaver v. Graham*, 450 U.S. 24, 101 S.Ct. 960, 67 L.Ed.2d 17 (1981))
[511] Wayne R. LaFave: Criminal Law (2010), p. 116. Application of the ex post facto prohibition would arguably be incompatible with the functioning of common law. See Wayne R. LaFave: Criminal Law (2010), p. 116, FN 8.
[512] Wayne R. LaFave: Criminal Law (2010), p. 122
[513] Wayne R. LaFave: Criminal Law (2010), p. 122
[514] Wayne R. LaFave: Criminal Law (2010), p. 122, FN 52 (citing *Bouie v. City of Columbia*, 378 U.S. 347, 84 S.Ct. 1697, 12 L.Ed.2d 894 (1964))
[515] Wayne R. LaFave: Criminal Law (2010), p. 122. However, it appears that judicial decisions may have retroactive effect if the conduct in question is malum in se. See Wayne R. LaFave: Criminal Law (2010), p. 123 and FN 58 on the same page. See also Wayne R. LaFave: Criminal Law (2010), p. 107 (in terms of whether to follow a previous, but erroneous precedent, invite the legislature to change the rule prospectively, or overrule the precedent. An Oregon court "made a distinction between crimes *mala in se* […] and crimes only *mala prohibita*; a person who commits a crime with "a consciousness of wickedness" in doing it has no right to the benefit of *stare decises*.")
[516] Wayne R. LaFave: Criminal Law (2010), p. 123-124

simple and natural one".[517] That is, the way in which a statute may be construed can reasonably be foreseen, and thus some warning is provided.[518]

5.3.2 The void-for-vagueness doctrine

Above, in the discussion of sources of law, and the role of international law in US law, I cited the US Constitution when stating that the Constitution is the supreme law of the land. The US Constitution is at the top of the hierarchy in terms of sources of law. All legislation, both state and federal, must comply with the Constitution. If legislation does not comply with the Constitution, the legislation is unconstitutional and void. The specific topic of this section is the doctrine called "void-for-vagueness". The doctrine addresses unconstitutional uncertainty in statutes and it derives from the due process clauses under the Fifth and Fourteenth Amendments to the US Constitution.[519] The Fifth Amendment guarantees due process in the federal arena while the Fourteenth Amendment guarantees due process in the state arena.[520] The void-for-vagueness doctrine addresses at least two due process concerns; fair notice, and guarding against arbitrary and discriminatory enforcement.[521] (Additionally, a statute must provide sufficient breathing space for First Amendment rights.[522])

Vagueness in statutes is framed as a constitutional issue, and as such, a statute that is void-for-vagueness is unconstitutional and, thus, can be struck down by the courts.[523] Substantive due process under the Fifth Amendment requires that Congress "be reasonably definite in declaring what conduct is criminal."[524] The clarity requirement addresses two concerns, as mentioned earlier: first, that the regulated have notice and, thus, can foresee the legality or illegality of their acts, and second, providing guidance to those enforcing the law to prevent arbitrary and discriminatory enforcement of the law.[525] The void-for-vagueness doctrine "is the operational arm of legality."[526]

---

[517] Wayne R. LaFave: Criminal Law (2010), p. 125 (citing Freund, The Supreme Court and Civil Liberties, 4 Vand.L.Rev. 533, 540 (1951))
[518] Wayne R. LaFave: Criminal Law (2010), p. 125
[519] Wayne R. LaFave: Criminal Law (2010), p. 108
[520] Wayne R. LaFave: Criminal Law (2010), p. 109
[521] *FCC v. Fox Television Stations, Inc.*, 567 U.S. XXX (2012), citing *Grayned v. City of Rockford*, 408 U.S. 104, 108-109 (1972)
[522] Wayne R. LaFave: Criminal Law (2010), p. 110. See also *FCC v. Fox Television Stations, Inc.*, 567 U.S. XXX (2012) citing *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870-871 (1997) ("The vagueness of [a content-based regulation of speech] raises special First Amendment concerns because of its obvious chilling effect.")
[523] Markus Dirk Dubber: Oxford Handbook of Comparative Law, p. 1316, and Wayne LaFave: Criminal Law, p. 109
[524] Wayne R. LaFave: Criminal Law (2010), p. 147-148
[525] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws, 80 Denv. U. L. Rev. 241 (2002), p. 244-245.

"The connection to legality is obvious: a law whose meaning can only be guessed at remits the actual task of defining criminal misconduct to retroactive judicial decisionmaking."[527]

Regarding indeterminacy, the question is two-pronged. The degree of indeterminacy must be evaluated, and then it must be evaluated whether the indeterminacy is acceptable in the given context.[528] Thus, indeterminacy is more of a sliding scale than an exact math. This comes as no surprise. However, criminal provisions tolerate much less indeterminacy than civil provisions.[529] But the most suspect type of indeterminacy is that which encroaches upon constitutional rights.[530] These are questions regarding limits as to what conduct the legislature can criminalize (in light of protected conduct), how much discretion can be granted to those enforcing the law (police officers, prosecutors) and to the courts, and it is a question of foreseeability (the regulated person's ability to adjust his conduct to the rules beforehand).[531] At the center of all these questions is clarity (specificity) insofar as a statute exists. The clearer and more precise a criminal provision is defined by the legislature, the less discretion it grants to other branches of the state and the more likely it is that the regulated persons can plan their conduct in accordance with the law. Of course, where no legislative criminalization has taken place, but rather a matter of judicial creation of crimes, it makes no sense requiring clarity since clarity is a qualitative aspect of the text of an already existing rule. Fair notice, however, relates to the predictability of the application of the rule. Clarity and foreseeability, whilst being closely related, are not synonymous.[532]

---

[526] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 196

[527] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 196

[528] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 196

[529] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws, 80 Denv. U. L. Rev. 241 (2002, p. 249

[530] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 196

[531] In the past, the Supreme Court had invalidated several laws, not because they interfered with protected conduct, but because the criminal statute bore no substantial relation to injury to the public. Such a finding would prevent the legislature from "trying again" unless societal circumstances change and a need for protecting the public from the conduct in question arises. This practice has been all but abandoned in the federal arena, with the Court finding itself on more solid ground by rather finding an interference with constitutionally protected conduct (even if that requires recognizing "penumbral rights" that do not follow directly from the language of the Bill of Rights) than passing judgment upon the wisdom of the legislature's policy choices. See Wayne R. LaFave: Criminal Law (2010), p. 149 et seq.

[532] As pointed out by Baumbach in terms of Danish law in Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 159

It follows from the Fifth Amendment to the US constitution that a criminal statute must be declared void for vagueness if "men of common intelligence must necessarily guess at its meaning and differ as to its application."[533] It means that if a criminal statute is vague enough, it is unconstitutional. One can wonder, though, how vague the language must be for a statute to become unconstitutionally vague, and whether, and how, lesser cases of vagueness can be "cured" by way of construction. In examining whether a statute is vague, the statute must be tested as it has been construed by courts.[534] The statutory text can therefore be vague in and of itself, but case law may have cured the vagueness. It should be noted that the courts start testing the statute under the presumption that it is constitutional.[535]

The void-for-vagueness doctrine is not limited to fair warning cases. Guarding against arbitrary and discriminatory enforcement has also been named as a basis of the void-for-vagueness doctrine.[536] Also a basis, is the need for sufficient breathing space for First Amendment rights.[537]

Summarily, the void-for-vagueness doctrine targets vague statutes. The consequence of a statute conflicting with this due process protection is unconstitutionality, and thus, invalidation of the statute.

The question is when a statute is so vague as to warrant invalidation. Fair notice and providing sufficient guidelines to the administrators of the law are ostensibly two independent prongs. Hence, a statute can be unconstitutional because it does not provide fair notice to the regulated, or, it can be unconstitutional because it authorizes arbitrary and discriminatory enforcement. A statute can also fail on both tests.

Whether a statute can survive scrutiny cannot be easily predicted. The void-for-vagueness doctrine does not come with an owner's manual, so to speak. As one commentator describes the appearance of the concept of vagueness: "I know it when I see it".[538]

---

[533] Wayne LaFave, Criminal Law, p. 109, citing Connally v. General Constr. Co., 269 U.S. 385, 46 S.CT. 126, 70 L.Ed. 888 (1939)
[534] Wayne LaFave, Criminal Law, p. 109, citing Winters v. New York, 333 U.S. 507, 68 S.Ct. 665, 92 L.Ed. 840 (1948)
[535] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 247
[536] Wayne LaFave, Criminal Law, p. 110
[537] Wayne LaFave, Criminal Law, p. 110
[538] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 214, p. 243

It is important to differentiate between ambiguity and vagueness. Ambiguity and vagueness are sometimes used interchangeably to convey general uncertainty. Courts are not necessarily consistent in their use of the terms, but one term is relevant to the vagueness doctrine and the other is not.

5.3.2.1 Ambiguity vs. vagueness

Ambiguity and vagueness are words that are often used interchangeably. In fact, one usage of the word ambiguity equates it to vagueness and uncertainty. Rather in this particular context, mindful of the irony that the word ambiguity itself is ambiguous, ambiguity is used in the sense that a word has two or more meanings; for example the word "light" (light as opposed to heavy, or light as opposed to dark). Legal language can be ambiguous and legal language can be vague. When a provision is ambiguous, it has more than one linguistic meaning, and its legal effect depends on which linguistic meaning is accepted by the courts. We use *interpretation* to resolve ambiguity and determine the linguistic meaning of the text, that is, its *semantic content*.[539] The context of the ambiguous word in a legal text will usually clarify whether the word takes on one or the other of various possible meanings. However, if the legal text does not provide enough context to choose between possible meanings, interpretation cannot resolve the ambiguity.[540]

When a provision is vague, the vagueness indicates that borderline cases exist – i.e. there are cases where the provision may or may not apply.[541] We use *construction* to resolve vagueness[542] "when the information conveyed by the text itself is insufficient to decide an issue, but the issue still must somehow be decided."[543] Construction gives the vague language *legal content*.[544] For example, the doctrines on "time, place, and manner" under the First Amendment. "Time, place and manner"

[539] Lawrence B. Solum: The Interpretation-Construction Distinction (2010), 27 Constitutional Commentary 95-118, p. 98
[540] Lawrence B. Solum: The Interpretation-Construction Distinction (2007), 27 Constitutional Commentary 95-118, p. 102
[541] Lawrence B. Solum: The Interpretation-Construction Distinction (2010), 27 Constitutional Commentary 95-118, p. 97-98
[542] Lawrence B. Solum: The Interpretation-Construction Distinction (2010), 27 Constitutional Commentary 95-118, p. 98
[543] Randy E. Barnett: Interpretation and Construction (2011), 34 Harv.J.L. & Pub. Pol'y 65-72, p. 69
[544] Lawrence B. Solum: The Interpretation-Construction Distinction (2010), 27 Constitutional Commentary 95-118, p. 98-99

restrictions do not follow from the text of the Constitution, but the doctrines are a way of putting First Amendment rights into effect.[545]

Some provisions, however, cannot be saved by construction.

To indulge in a brief example from the section on article 7 ECHR, recall the case *Liivik v. Estonia*. A criminal provision interpreted as prohibiting mere creation of risk of causing significant moral damage to the interest of the state, where the moral damage (a term itself fraught with vagueness) was considered "significant" based solely on the fact that the defendant was a high-ranking official. *Liivik* is arguably a prime example of a case involving a provision that relies too much on judicial construction (as well as creativity), or at least has been construed by the courts in a manner that rendered the provision entirely too vague, since any person in Liivik's position would be unable to defend himself or, arguably, even avoid conviction, unless the prosecution decided within its discretion not to pursue the case.

5.3.2.2 Vagueness vs. overbreadth

Decker explains the difference between vagueness and overbreadth in the following way:

"If a party challenges an enactment based on the assertion that one cannot determine whether the regulation intrudes upon otherwise "innocent terrain," then the complaint is one of vagueness. On the other hand, if a challenge is based on an objection that the regulation does, in fact, intrude into territory where it does not belong, then the claim is one of overbreadth."[546]

Overbreadth in this context relates to constitutionally protected conduct, typically conduct protected by the First Amendment. In cases of facial overbreadth the courts examine whether the provision reaches a substantial amount of protected conduct.[547] In other words, the statute is capable of producing a chilling effect on constitutionally protected conduct. "Facial" means that the entire statute is unconstitutional (as opposed unconstitutional "as applied" in a particular case). One of the important differences between attacking a statute on overbreadth grounds and vagueness grounds lies in that, with regard to *overbreadth*[548], a defendant can argue that the statute is capable of

[545] Randy E. Barnett: Interpretation and Construction (2011), 34 Harv.J.L. & Pub. Pol'y 65-72, p. 69. For example, one's right to broadcast one's opinions with a loudspeaker in the middle of the night in a residential neighborhood is not necessarily a desirable time, place and manner of exercising free speech, if other people's rights are taken into consideration.
[546] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 266
[547] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 266
[548] Facial overbreadth is merely included in this discussion for purposes of distinguishing between overbreadth and vagueness. Overbreadth, as discussed briefly in the above section on article 7 ECHR, is a question of balancing. If there

possible unconstitutional application to others even though his own conduct does not constitute protected conduct. In *facial vagueness* challenges, the defendant has to show that the statute is vague as applied to him as well as being vague "in all its applications".[549]

Another option is to challenge the statute on the grounds of its being vague "as applied". When a defendant claims that a statute is unconstitutionally vague as applied, it means that he claims the statute, that criminalizes the conduct with which he has been charged, did not define the conduct with sufficient clarity.[550] The court can only evaluate the statute *in light of the facts in the case before it*, not whether the statute is too vague to be applied in any case at all.[551] That is, the defendant whose conduct clearly falls within the scope cannot challenge the statute with reference to possible vagueness as applied to others, as he would have been able to had his challenge focused on "overbreadth" rather than vagueness. "Where an individual engages in conduct without any reasonable realization that it falls within the reach of a legal prohibition, that person may succeed with an as applied challenge."[552] When a statute is void as applied it generally means that although the provision's language does not clearly differentiate between illegal and legal conduct, it still has general value that outweighs the harm of the uncertainty. With respect to marginal conduct, the statute can then be declared void as applied.[553]

LaFave contrasts the two, vagueness and overbreadth, by pointing out the discrete messages sent by courts. If a court finds a statute void for vagueness, it means that it is uncertain to which extent the legislature intended to exercise its power, and that the uncertainty is such that it is for the legislature to cure it, not the courts.[554] The message to the legislature is "try again".[555] However, if the legislature has overstepped its power to create crimes – such as crimes that infringe upon

---

is no overlap between, on the one hand, conduct that is positively protected by law from government interference and, on the other hand, conduct that has been criminalized, it makes little sense to take about "over"-breadth, since no

[549] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 280

[550] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 280

[551] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 280

[552] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 282

[553] Congressional Research Service Annotated Constitution, p. 1747 (Due Process, Fourteenth Amendment). Available at http://www.law.cornell.edu/anncon/html/amdt14efrag2_user.html. Last accessed on 21 February 2015.

[554] Wayne R. LaFave: Criminal Law (2010), p. 138

[555] Wayne R. LaFave: Criminal Law (2010), p. 138

constitutionally protected conduct – the message to the legislature is "hands off".[556] "Try again" means that the legislature can try again, but must define with greater care the conduct it seeks to criminalize, whereas "hands off" definitively excludes the conduct from the statute's scope and the legislature cannot again try to include the conduct, unless the legislature can make a stronger demonstration of the need to interfere with the protected conduct.[557]

5.3.2.3 Fair notice

Fair notice means that the defendant could have found out, had he wanted, whether his acts or omissions would trigger the application of the statute in question. A statute must therefore be sufficiently precise so as to draw a reasonably clear line between illegal and legal conduct.[558] "[A] statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application, violates the first essential of due process of law."[559] In other words, a statute must provide fair notice and cannot be "so standardless that it authorizes or encourages seriously discriminatory enforcement."[560]

The clarity requirement regarding criminal law is fundamental in terms of the Fifth Amendment due process clause.[561] This requirement necessitates "the invalidation of laws that are impermissibly vague."[562] "Undue vagueness in the statute will result in it being held unconstitutional, whether the uncertainty goes to the persons within the scope of the statute, the conduct that is forbidden, or the punishment that may be imposed."[563] [564] (citations omitted) However, not just any vagueness renders the statute unconstitutional.

---

[556] Wayne R. LaFave: Criminal Law (2010), p. 139
[557] See Wayne R. LaFave: Criminal Law (2010), p. 139
[558] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 248
[559] *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)
[560] *FCC v. Fox Television Stations, Inc.*, 567 U.S. XXX (2012), citing *United States v. Williams*, 553 U.S. 285, 304 (2008)
[561] *FCC v. Fox Television Stations, Inc.*, 567 U.S. XXX (2012)
[562] *FCC v. Fox Television Stations, Inc.*, 567 U.S. XXX (2012)
[563] Wayne R. LaFave: Criminal Law (2010), p. 109
[564] The same principle applies to common law crimes and sanctions in administrative regulations, as noted by Wayne R. LaFave in Criminal Law (2010), p. 109

First and foremost, the fact that a statute is vague, to a degree, on its face is not sufficient in and of itself.[565] The statute is tested with its judicial gloss. This means that the statute is tested in light of how it has been construed by courts.[566] Thus, the courts can "cure" the vagueness, and the statute can escape unconstitutionality even though its language is vague seen in isolation. The courts can sufficiently clarify vague language, and therefore provide the necessary clarity that both gives fair notice to the regulated and gives sufficiently clear guidelines to those enforcing the laws to avoid arbitrary or discriminatory enforcement. Furthermore, language that may seem unclear on its face to the average individual may also have an established meaning in common law or in other legislation.[567] A statute can thus very well be vague on its face and incomprehensible to the average person and yet be constitutional when it is read in light of other sources providing clarification.[568] However, those cases may require the average individual to seek out legal advice.[569] For that reason, notice can be hard to come by, since that notice may only reveal itself after extensive research of precedents – more akin to notice to the individual that he must seek legal advice[570], i.e. notice that his conduct may be illegal.[571]

Comparable to the foreseeability requirements under article 7 ECHR, the fair notice requirement is not universally the same for all statutes. There is a greater tolerance for vagueness if the statute in question regulates businesses rather than individuals.[572] Greater precision is also required in criminal statutes than in civil statutes, because civil consequences are less severe.[573] Scienter requirements may reduce vagueness where the statute requires that the defendant is aware of his

[565] John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 207
[566] Wayne R. LaFave: Criminal Law (2010), p. 109. See also *Winters v. New York*, 333 U.S. 507 (1948).
[567] Wayne R. LaFave: Criminal Law (2010), p. 110
[568] Wayne R. LaFave: Criminal Law (2010), p. 110. See also John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 207.
[569] Wayne R. LaFave: Criminal Law (2010), p. 110
[570] See generally John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 208
[571] Arguing against so-called "lawyer's notice", see John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 211
[572] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 248-249 (citing Vill. Of Hoffmann Estates, 455 U.S. at 498)
[573] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 249

conduct's illegality.[574] Finally, if the statute might interfere with constitutionally protected conduct, the notice requirement is less likely to be fulfilled.[575]

As Jeffries explains it[576], if the purpose of requiring the legislature to give fair notice of what is forbidden, and that ignorance of the law is no excuse, surely there is an assumption that what is not clearly forbidden is permitted. But if the law is fraught with uncertainty or practically inaccessible, then the "ignorance of the law is no excuse"[577] mantra is converted into a risk-based game where illegality is presumed. Jeffries explains it this way in order to demonstrate that fair notice, and the clarity requirements associated with it, seems to inconsistent with the policy that ignorance of the law is no excuse. This is eerily similar to the ECtHRs references to risks of possible prosecution in grey areas of the law; Ashworth's thin-ice principle. However, Jeffries expressly states that this kind of "notice" should not be sufficient to trigger criminal liability, rather he notes that the absence of signals to the citizen that he may risk liability should preclude liability.[578]

5.3.2.4 Guarding against arbitrary and discriminatory enforcement

This requirement is also referred to as "ascertainable standard of guilt". This aspect of legality is considered the more important aspect of the vagueness doctrine.[579] The aspect concerns itself not with notice to the citizens as such, but with requiring the legislature to provide law enforcement with minimal guidelines.[580] Even when the defendant is on notice, those enforcing the law may have unchecked discretion to enforce the law as they see fit. An example of such discretion is embodied in a statute that requires a person who has been lawfully stopped to provide "credible and

---

[574] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (220), 80 Denv.U.L.Rev. 241, p. 249

[575] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 249

[576] See John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, pp. 209-210

[577] Of course, if this were a legal excuse for violation of the law, then the law applying would be the law as subjectively understood by that individual rather than what the law objectively is to everyone else. See John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 2010, note 57

[578] See John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 211, note 58

[579] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 253

[580] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 253

reliable" identification.[581] Those enforcing the law, in the first instance the police officers, can arbitrarily decide whether identification lives up to being "credible and reliable". When the legislature does not include determinate standards in criminal provisions those enforcing the law and the triers of fact have unchecked discretion.[582] That is, an absence of a legally fixed standard leaves the trier of fact to decide on a case-by-case basis whether the conduct in question is reasonable or not.[583] Therefore, the statute or a specific provision in the statute allows, or even encourages, arbitrary and discriminatory enforcement of the law because the subjective judgment of the enforcer controls the conduct's criminality entirely unaided by objective norms.[584] That is, the law is "wholly lacking in 'terms susceptible of objective measurement.'"[585] Such laws are invalidated because they are incompatible with due process requirements and thus unconstitutional.[586]

Allowing the application of the void-for-vagueness doctrine in First Amendment cases, even where the challenged statute is not vague as applied to the defendant, is a special instance of guarding protected conduct from arbitrary interference from those enforcing the law.[587]

5.3.2.4.1 Discretion and the rule of law

Clearly not any level of discretion granted to those enforcing the law calls for voiding the statute in question. The legislator regularly grants the administrators of the law discretion.[588] LaFave mentions the term "reasonable" as an example.[589] A standard of reasonableness does not necessarily

---

[581] *Kolender v. Lawson*, 461 U.S. 352 (1983). See also Wayne R. LaFave: Criminal Law (2010), p. 113, footnote 50. Other examples are *Papachristou v. City of Jacksonville*, 405 U.S. 156 (1972) and *City of Chicago v. Morales*, 527 U.S. 41 (1999). See also John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 253 et seq.

[582] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 253

[583] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241, p. 253-254. Discussing this point from a rule of law view, see John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 214

[584] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 253

[585] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 253 (citing Keyishian v. Bd. Of Regents, 385 U.S. 589, 604 (1967))

[586] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 253

[587] See John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 217

[588] Wayne R. LaFave: Criminal Law (2010), p. 114

[589] Wayne R. LaFave: Criminal Law (2010), p. 114

render a statute void for vagueness.[590] The principle of necessity may lend support to upholding a statute that leaves room for arbitrariness in its enforcement because it is not possible to narrow the language without rendering the statute too rigid and difficult to administrate, or, on the other hand, necessity could perhaps necessitate rewording of the language to lower the risk of arbitrary enforcement.[591] Possibly, less risky wording could yield the same result. Therefore, whether a certain degree of discretion can be upheld as constitutional may depend on whether that degree of discretion is necessary and appropriate.[592]

The rule of law is at the heart of the principle of legality and thus the void-for-vagueness doctrine.[593] Following Jeffries' definition of the rule, "[t]he rule of law signifies the constraint of arbitrariness in the exercise of government power. In the context of the penal law, it means that the agencies of official coercion should, to the extent feasible, be guided by rules – that is, by openly acknowledged, relatively stable, and generally applicable statements of proscribed conduct. The evils to be retarded are caprice and whim, the misuse of government power for private ends, and the unacknowledged reliance on illegitimate criteria of selection. The goals to be advanced are regularity and evenhandedness in the administration of justice and accountability in the use of government power. In short, the "rule of law" designates the cluster of values associated with conformity to law by government."[594]

As Jeffries also points out, the rule of law is a sliding scale rather than a binary state. Discretion plays a role in every legal system.[595] If a statute is too rigid, it may be difficult to administrate the statute in practice or it may lose its usefulness to combat the crime it targets. If a statute leaves too much discretion, the administrators of the law can arrest whomever they want. However, the rule of law is not a rule of equality. Strict adherence to the rule of law says nothing about the subject matter

---

[590] Wayne R. LaFave: Criminal Law (2010), p. 114, footnote 54, citing *State v. Wilchinski*, 242 Conn. 211, 700 A.2d 1 (1997)
[591] Wayne R. LaFave: Criminal Law (2010), p. 114
[592] "The power to define a vague law is effectively left to those who enforce it, and those who enforce the penal law characteristically operate in settings of secrecy and informality, often punctuated by a sense of emergency, and rarely constrained by self-conscious generalization of standards. In such circumstances, the wholesale delegation of discretion naturally invites its abuse, and an important first step in constraining that discretion is the invalidation of indefinite laws." John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 215
[593] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 212
[594] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 212-213
[595] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 213

addressed by a statute. A statute might even authorize discrimination of the worst kinds, and its application would still conform to the rule of law.[596]

5.3.3 The Rule of Lenity

As mentioned in the section on ambiguity vs. vagueness, ambiguity entails that a provision is somewhat precise but lends itself to two or more discrete readings. The rule of lenity, also known as the rule of strict construction, and sometimes referred to as junior version of the void-for-vagueness doctrine[597], requires that the ambiguity in a criminal provision is resolved in favor of the defendant.[598] Thus, for the rule to apply, an ambiguity must be present in the statute. The rule of lenity is not one derived from the Constitution, nor is it directly derived from the principle of legality, although it may be considered to implement the ideal of legality.[599] The rule of lenity has been said to further the purpose of due process and the idea that only the legislature can define crimes.[600] It only applies to criminal statutes.

The Supreme Court has held that the rule of lenity applies only in cases where the statute is inflicted with a "grievous ambiguity or uncertainty"[601], although in its original form it applies to all ambiguities in criminal statutes. Like the ECtHR, the US Supreme Court has also recognized that most statutes are ambiguous to some extent.[602] Furthermore, the Court has indicated that the rule of lenity is a rule of last resort, when all other interpretive tools have been exhausted and the court can no more than guess at what Congress intended.[603] When applied, the rule cannot be used to force a

[596] John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, p. 213, footnote 64. Jeffries uses apartheid as an example.
[597] John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 200 and John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 262
[598] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 262
[599] John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 185
[600] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 262
[601] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 264
[602] Muscarello v. United States, 524 U.S. 125, 138 (1998)
[603] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 264

nonsensical or overly strict construction.[604] These reservations to the original form of the rule, all narrow its potential applications.

A statute's applicability to situations that ostensibly were not anticipated by the legislature does not constitute ambiguity, but rather breadth.[605] Over-inclusion does not equate ambiguity, and thus does not require the application of the rule of lenity.

The rule of lenity appears to have fallen into disuse, and is not favored e.g. by the Model Penal Code, in addition to some states have, by way of statute, expressly excluded its application.[606] One aspect of the critique of the rule centers on its ability to run contrary to legislative intent.[607]

The rule of lenity's apparent hardline approach to ambiguity may be explained from a historical perspective. The rule originated in English law in the 18th century where capital punishment was imposed for a vast number of crimes, even minor ones. Strict construction of criminal statutes was thus a matter of resolving ambiguities in favor of life rather than death[608] and the English courts would in fact strive to find ambiguities so that they were required to resolve it in favor of the defendant, sparing his life.[609] However, the rule has been cited in the US at least as far back as 1820 when Chief Justice Marshall cited it in *United States v. Wiltberger*.[610] The apparent rationale of the rule in English law was ostensibly reinvented in US law in that the rule of lenity is often said to further due process, separation of powers and sometimes also as furthering the rule of law.[611] Commentators have criticized those rationales and arguably rather clearly shown that they do not justify the rule of lenity, because strict application of the rule of lenity in all cases of ambiguity can lead to results that contradict those rationales.[612] In other words, the rule's critics argue either that it

---

[604] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 264
[605] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 265
[606] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 265
[607] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 265
[608] John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 198, Andrew Ashworth and Jeremy Horder: Principles of Criminal Law (2013), p. 67 and Wayne R. LaFave: Criminal Law (2010), p. 93
[609] Wayne R. LaFave: Criminal Law (2010), p. 93, FN 26 (citing Hall, Strict or Liberal Construction of Penal Statutes, 48 Harv.L.Rev. 748, 751 (1935))
[610] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2420
[611] See analysis in e.g. John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, pp. 189-245
[612] See further on the critique in Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2424 et seq.

is applied inconsistently[613] or randomly, or that it has ceased to be used, with many of its critics willing welcoming its apparent demise.[614]

Today, the rule, both in US law and English law, its critics argue, only survives as additional padding for a conclusion already arrived at through other means, and thus its reference appears pro forma[615], rather than being the deciding or an influential factor for the outcome of the case.[616] Additionally, due to the rule requiring an ambiguity in the statute, the courts may see a need to "manipulate the threshold determination of ambiguity in order to avoid applying the old rule [of lenity]."[617]

However, a study of the Rehnquist court's application of the rule argues that a new, but narrower, rule of lenity has gradually emerged, as the traditional rule of lenity has weakened since the 1970s.[618]

The study concludes that the rule of lenity has indeed been decisive, and not just cited pro forma, in a small but significant number of cases.[619] However, not in its traditional form. In the study, it is argued that the cases "reflect the Court's desire to avoid the criminalization of innocent conduct."[620] Innocent conduct, according to the study, involves situations where "the defendant does not even need to be aware of the factual circumstances that make her actions criminal to be convicted or if the defendant must be aware of the relevant facts but need not be aware of their legal significance. Actions that are malum in se provide notice of wrongfulness by their very nature. When the conduct at issue is only malum prohibitum, however, this notice can only be guaranteed if the statute incorporates knowledge of illegality […] or wrongfulness […] into the definition of the offense."[621]

[613] See e.g. Markus Dirk Dubber: Comparative Criminal Law, p. 1314
[614] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2424
[615] John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 199
[616] Andrew Ashworth and Jeremy Horder: Principles of Criminal Law (2013), p. 68 and John Calvin Jeffries: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, p. 198-199
[617] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2440
[618] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2423-2424
[619] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2421
[620] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2431
[621] Note, The New Rule of Lenity (2006), 119 Harv.L.Rev. 2420, p. 2435

5.3.4 Summary

As with article 7 ECHR, the void-for-vagueness doctrine does not demand absolute certainty, nor does it require impossible standards of clarity. Figuring out what degree of certainty is required seems to be a case of "I know it when I see it", rather than being based on objective tests. However, in US law, those laws that have succumbed to a vagueness attack, are those which do not provide a reasonably clear line between legal (including constitutionally protected conduct) and illegal conduct, those laws that require no proof of scienter, those prescribing criminal penalties rather than civil penalties, and those where the regulated are individuals rather than business entities.[622] The fair notice required is a matter of degree, rather than a "one size fits all" standard. However, those statutes that allow or encourage arbitrary and discriminatory enforcement in that they leave the enforcers or the triers of fact to determine, subjectively in absence of an objective standard, the applicability of a statute, are those most suspect and least tolerated.

Statutes which are "merely" ambiguous, but not vague, are generally not unconstitutional. At least insofar as the ambiguity can be resolved. If the ambiguity is of the grievous kind, it calls for the application of the rule of lenity, although ostensibly only if all other interpretative sources have failed to resolve the ambiguity; the rule of lenity as a last resort. Alternatively, if there is indeed a new rule of lenity, that rule will serve to strictly construe statutory language in order to protect innocent conduct, ostensibly providing for a more coherent and consistent rule of lenity.

5.4 Brief overview

	ECHR	**US Law**	**Danish Law**
Foreseeability / fair notice/warning	(Article 7) Foreseeability is a qualitative requirement along with accessibility.	(Void-for-vagueness doctrine) Fair warning / fair notice. Follows from the due process clause of the Fifth Amendment to the	(Criminal Code § 1, partially) Follows from the underlying rationale of § 1, but the text of § 1 still allows for punishment

[622] John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv.U.L.Rev. 241, p. 252

		Constitution. (Courts) Retroactivity is prohibited under the Constitution. (Legislature)	of wholly analogous conduct, and it does not prohibit retroactive criminalization occurring after the conduct but before adjudication. However, article 7 ECHR supplements the § 1 legality requirement in those respects.
Degree of foreseeability	Varies. Lesser degree acceptable for statutes regulating businesses. (Article 7 does not apply to civil statutes, as opposed to the void-for-vagueness doctrine.) Also depends on the subject matter (e.g. lesser precision accepted concerning terrorism statutes).	Varies. Lesser degree acceptable for statutes regulating businesses and civil statutes. Statutes lacking mens rea requirement generally disfavored. May turn on whether conduct is malum in se or malum prohibitum.	Follows from article 7 ECHR. Only subject to non-binding standards of "good draftsmanship". (Mens rea required is "intentional" by default according to the criminal code § 19, unless lower degree is specified. Thus typically no mens rea issue. The legislature is not technically prohibited from passing criminal laws lacking mens rea. Mens rea for special legislation negligence

			unless specifically limited to intentional acts.)
Foreseeability requirement can also be met if legal advice needed to determine scope of application	X	X	X (Follows from article 7 ECHR)
Guard against arbitrary and discriminatory enforcement	(Article 7 ECHR) Follows from Camilleri and Liivik that article 7 ECHR prohibits excessive prosecutorial (in Camilleri, the discretion was not subject to judicial review) and/or excessive judicial discretion (Liivik).	(Void-for-vagueness doctrine) "Ascertainable standard of guilt" required of the law. Law has to provide reasonably clear lines between lawful and unlawful conduct. Those laws "which turn on language calling for the exercise of subjective judgment (of the enforcer) unaided by object norms" and/or "leaves judges and jurors free to decide, without any legally fixed standards, what is prohibited and what is not in each particular case." (Decker, p. 253)	Underlying rationale of the criminal code's § 1. Also follows from article 7 ECHR.

How is the statute tested	(Article 7 ECHR) As interpreted by national courts. Not tested facially, but in light of case law.	(Void-for-vagueness doctrine) With its judicial gloss. Not facially.	Follows from article 7 ECHR.

5.5 Conclusions

In this chapter I have addressed the ways the principle of legality, nullum crimen, nulla poena sine lege, is operationalized in two legal systems and in the ECHR (and touching briefly upon EU law). Even though terms may differ, whether the root of the idea for protection derives explicitly from the Enlightenment or not, and the way the protection is realized differs, the core protection is more or less the same. We do not desire retroactive criminalization. We do not desire incomprehensible laws that take us by surprise. We do not desire arbitrary and discriminatory enforcement of laws by way of wholesale legislative delegation of discretion. We share these values across cultures and legal systems. The difference lies in the extent of protection; that is, when on the sliding scale we find that those values are offended.

Although the abovementioned protection guarantees us fair notice, and protects us against unconstrained exercise of governmental power, these two aspects of protection say nothing about the substantive content of a criminal provision. These protections only ensure due process under the law during the application of the law; that is, protection against procedural discrimination and arbitrariness at the administrative and judicial level. The principle of legality does not protect against unreasonable, undesirable or unjust substantive content; that is, discrimination and/or overcriminalization at the legislative level (be it explicitly stated or a natural consequence of the language). Even though clarity promotes notice, clarity does not necessarily constrain discretion, and clarity does not scrutinize the subject matter of a provision. Not all "innocent" and desirable behavior is constitutionally protected conduct. That is even truer in Denmark where the Danish Constitution enshrines very few fundamental rights compared to the United States Constitution. When a statute's language reaches "normally innocent" conduct, the question of whether the language allows the enforcers of the law to differentiate between illegal and legal conduct, hinges on the presumption that the legislator did not intend for the "normally innocent" conduct to be

included. That is, it rests on a presumption that there are in fact legal acts that fall within the scope of the statute, rather than a presumption that all that the language can cover is intended to be covered.

6 THE COE'S CONVENTION ON CYBERCRIME

6.1 Brief overview of the substantive articles

This dissertation focuses on crimes involving unauthorized access to a computer. Unauthorized access, or illegal access, is addressed by a single article in the Convention on Cybercrime. Although the scope of the substantive part of the Convention is much broader than illegal access, illegal access often, but not necessarily, precedes many of the other substantive crimes, such as illegal interception and data interference. Articles 2-6 address attacks against computers; i.e. the computer is the target of the attack. The Convention also covers some traditional crimes committed through use of computers, such as forgery covered by article 7 and fraud covered by article 8, and also content-related crimes such as child pornography (article 9) and copyright protected material (article 10). These content-related crimes and traditional crimes whether committed through use of computer or not, are not directly relevant to this dissertation apart from situations where unauthorized access statutes are used as a proxy to prosecute undesirable use or possession of specific content. Of interest to this dissertation is article 2 which requires criminalization of illegal access to computer systems. The article states:

"Each Party shall adopt such legislation and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

Chapter 1 of the Convention defines the terms "computer system", "computer data", "service provider" and "traffic data" in article 1, litra a, b, c and d, respectively. The two terms defined in chapter 1 that are used in article 2 are "computer system" and "computer data". They are defined in article 1(a) and (b), respectively:

(a) "[For the purposes of this Convention:] "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;"

(b) "[For the purposes of this Convention:] "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;"

Chapter 2, section 1 (articles 2-6), which contains substantive criminal law, requires the parties to criminalize a number of offences. Articles 2-6 cover offences that are labeled as "offences against

the confidentiality, integrity and availability of computer data and systems" – i.e. offenses where the computer is the target. These offenses comprise illegal access (article 2), illegal interception (article 3), data interference (article 4), system interference (article 5) and misuse of devices (article 6)[623]. Arguably, article 6 on misuse of devices does not as such describe an attack against a computer, but rather article 6 is aimed at banning tools intended to be used to commit one of the attacks against computers described in articles 2-5. Possession of a device covered by article 6 (including software) primarily for the purpose of committing offences in articles 2 through 5 is to be criminalized if there is intent to use (article 6 (1b)). Production, sales, distribution,[624] etc. of such devices is also required to be criminalized. Article 6(3) allows parties to exempt from the scope of the offense mere possession of devices as long as there is no intent to sell or distribute access codes, passwords and similar data that are covered by article 6(1)(a)(ii), whilst article 6(2) makes it clear that outside the scope of article 6 falls possession, sale, distribution, use etc. of article 6 devices if the purpose is not the committing of any of the offenses in articles 2-5; article 6(2) exempts from the scope situations such as where the possession is for the purposes of authorized testing or protection of a computer system or other similar situations where the purpose is not to commit a crime as defined in articles 2 through 5.

As noted above, the main focus of this dissertation is the lack of certainty with respect to the scope of hacking statutes due to the legislatures' use of terms the scope of which, essentially, is understood, or fully comprehended, by no one.[625] The specific elements of article 2 are subject to further discussion in the coming chapters that address the specific elements central to hacking statutes, namely "access" and "without right"/"authorization". Before diving into the definitions in the subsequent chapters, I will take a look at the reasons for drafting the Convention on

---

[623] Not surprisingly, the drafters had trouble deciding how to approach criminalization of "misuse of devices" because a lot of the software used for criminal purposes are also used for legitimate purposes by IT professionals. Including all devices would mean that the question as to whether an act is criminal hinged entirely on "intent", which was unacceptable to the drafters. Rather than opting for an extremely narrow, and perhaps rather impractical, approach that required a device to be exclusively designed for committing articles 2-5 offenses, a compromise lead to the approach that devices must be objectively designed or adapted primarily to commit articles 2-5 offenses. See explanatory report, para. 73. However, arguably, even this compromise does not guarantee the exclusion of dual-use devices from the scope of article 6, since a device may well have been designed for one purpose, but used by many for another purpose.

[624] Note that the explanatory report ostensibly indicates that the concept of "making available" should be read broadly, as the report notes in para. 72 that creating or compiling hyperlinks to devices covered by article 6 is also intended to be criminalized.

[625] See Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1598

Cybercrime; that is, an inquiry into the general purpose of the Convention and the interests protected by the Convention's article 2.

6.2 The General Purpose of the Convention's Article 2

Since the negotiations of the Convention lacked transparency[626], the Explanatory Report, which accompanied the Convention and was adopted by the Committee of Ministers of the Council of Europe, generally provides the highlights of the compromises made during the drafting of the Convention.

First off, the title under which article 2[627] is placed in the Convention is called "Offences against the confidentiality, integrity and availability of computer data and systems".[628] The title nicely sums up the interests protected by articles 2-6 collectively; namely, the CIA-triad as it is sometimes called in the IT security field (Confidentiality, Integrity and Availability). The Explanatory Report notably adds to this language that articles 2-6 are not intended "to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices."[629]

In accordance with the idea of the articles protecting confidentiality, integrity and availability, the Explanatory Report emphasizes that the threat of criminal law is secondary to implementation of effective security measures. However, as the language of article 2 indicates, circumvention of security measures is not required to trigger criminal liability.[630] And yet the Explanatory Report clearly shows that the drafters considered article 2 to cover "dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data."[631] The Report furthermore shows that the drafters intended to exclude access to publicly accessible systems from the scope of article 2.[632] Apart from a few very clear exemptions, such as the access to publicly accessible systems, from article 2's broad scope that the drafters seemingly agreed upon, the article's scope is not undisputed. The dispute concerning the scope of article 2 – and likely the

[626] The American Civil Liberties Union called the drafting process "closed, secretive and undemocratic". ACLU website "The Seven Reasons Why the Senate Should Reject the International Cybercrime Treaty"
[627] Article 6 is also placed under this title, but is excluded from the discussion since it does not fall within the scope of the dissertation.
[628] Title 1 of the Convention on Cybercrime
[629] The Explanatory Report, para. 43
[630] Such a narrower version of article 2 is optional, not mandatory.
[631] The Explanatory Report, para. 44
[632] The Explanatory Report, para. 47

reason for the general ambiguity concerning its scope, except for those few exceptions clearly stated in the Explanatory Report – is explicitly noted in the Explanatory Report. Those opposing the broad scope appear to have been concerned with those cases of unauthorized access where there was no danger created or where vulnerabilities in computers systems where discovered as a result of the unauthorized access.[633]

The scope of article 2 is generally unclear and disputed (apart from some clear examples of conduct intended to be excluded from the scope), and the Convention grants the signatories considerably broad discretion as to its implementation. The signatories are free to criminalize simple computer trespass[634], i.e. the bare-boned article 2, or the signatories can narrow the national criminalization of illegal access to instances where security measures were infringed, where the offender intended to obtain computer data or other types of dishonest intent, or where the access was gained remotely (from one system to another).[635] These additional elements and additional scienter requirements can result in national implementations the scope of which vastly differ, and yet, supposedly are the product of an international effort to "harmonize" domestic substantive criminal law elements to ease cooperation between countries and prevent creation of safe-havens for cybercriminals. Even if all signatories had implemented the basic version of article 2, the construction of the vague concepts used ("authorization" and "access") is highly unlikely to be uniform across the signatories' legal systems.

At least one commentator has criticized the Convention for being too vague on definitions and its terms too broad to be enforced.[636] Marion's critique seems to stem from the fact that that there is no guarantee of a uniform implementation and application of the Convention, nor even a guarantee of uniform interpretation of terms like "access" or "authorization/right", the definitions of which are critical in determining whether a person has committed a crime or not.

This presumption of lackluster harmonization appears to have a high degree of truth to it since there is clear disagreement and still ongoing dialog, even between the national courts within one signatory, as to the meaning of the terms, which has created a split between jurisdictions with regard to the application of the hacking statute, as shown in the following chapters on access and authorization with respect to outsiders and insiders.

---

[633] The Explanatory Report, para. 49; it is also noted in the same paragraph that the narrower approach comports with a 1989 report on computer crime and an OECD proposal from 1985.
[634] The term "computer trespass" is used in the Explanatory Report, para. 44
[635] See the Convention's article 2
[636] Marion: The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation, p. 705

7 EU LAW

In the early 2000s, in the wake of the negotiation, drafting and adoption of the Council of Europe's Convention on Cybercrime, the European Union slowly started to look towards harmonization of national criminal law provision on attacks against information systems. The Commission stated that attacks against information systems were a threat against the establishing of a safer information society and an area of freedom, security and justice.[637] Therefore, EU action was considered required.

Particularly, the Commission worried about organized groups of hackers, organized crime, serious attacks committed by individuals, and terrorism. The gaps and differences in national laws, the Commission argued, could hinder the fight against these types of high-tech crimes.[638]

7.1 The 2005 Framework Decision

The harmonization would take place through a framework decision. Council framework decisions are the constructs of the old pre-Lisbon treaty pillar system. The Council's (not to be confused with the Council of Europe, which is not an EU institution) framework decision on attacks against information systems originated in the old third pillar, as explained in the chapter on sources of law.

The goal of the Council's Framework Decision proposed by the Commission was to approximate Member State criminal law provisions, and improve law enforcement and judicial cooperation when dealing with attacks against information systems. Simultaneously, the proposal was meant to aid the EU in its fight against organized crime and terrorism.[639]

The Commission decided to follow the same approach as, and the framework is in fact to a large extent based on, the Council of Europe's Convention on Cybercrime; namely, the framework decision aimed to protect confidentiality, integrity and availability of information systems.[640]

Framework Decision 2005/222/JHA on attacks against information systems entered into force on March 16th 2005. The Framework Decision's articles 2 to 4 criminalized what was already required to be criminalized under the CoE's Convention on Cybercrime articles 2, 4 and 5; namely, illegal

[637] COM (2002) 173 final, p. 2
[638] COM (2002) 173 final, p. 7
[639] COM (2002) 173 final, pp. 7-8
[640] COM (2002) 173 final, pp. 8-9

access to information systems, illegal interference with information systems, and illegal interference with data, respectively.

Article 2(1) of the Framework Decision reads:

"Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor."

Like the corresponding article in the Convention, the Framework Decision's article on illegal access gave the Member States the option of only criminalizing illegal access when committed by infringing security measures.[641] Additionally, according to the Framework Decision, the Member States were afforded the option to criminalize only cases, which were not minor.[642]

In a 2002 proposal for the Framework Decision contained definitions and understandings of a concept "authorized person", which e.g. included exempting legitimate scientific research from the scope of the article 2.[643] This concrete exception did not make it into the 2005 Framework Decision. Similarly, the "illegal access" article proposed in 2002 was significantly narrower than the one in the final version, limiting the scope of article 2 to where the illegal access involved systems with specific protection measures, or the illegal access was committed with either the intent to cause damage or the intent to benefit economically.[644]

A few years later, in 2008, the Commission published its report on the implementation of the Framework Decision. In the report, the Commission criticized how the few Member States, which had chosen to exclude applicability to minor cases, had implemented that "minor case" limitation of the criminalization. The Member States had apparently added additional elements to the crime, for example, that the information obtained from the illegal access had to have been abused subsequently, or had added requirements of specific risks or damages. The Commission then clarified how it interpreted the concept of minor cases: "[T]he concept of minor cases must refer to cases where instances of illegal access are of minor importance or where an infringement of information system confidentiality is of a minor degree." [645] The four countries that had

[641] Article 2(2) gives the option of restricting the implementing national provision to cover only those acts committed by infringing a security measure.
[642] These options were meant to mirror the reservations allowed under the Convention on Cybercrime. See COM(2002) 173, p. 10
[643] COM(2002) 173, p. 11
[644] COM(2002) 173, p. 21
[645] COM(2008) 448 final, p. 4

implemented the "minor cases" limitation had therefore not implemented the illegal access article properly because they had added additional elements to the crime, where they instead ostensibly should have weeded out the minor cases on a case-by-case basis. The option of limiting the illegal access provision to cases that involved infringement of security measures had been applied by seven countries.

Furthermore, the Commission had reservations about the Danish implementation of articles 3 and 4 (illegal interference with information systems and illegal interference with data, respectively). Denmark had informed the Commission that these two articles were implemented via the Danish Criminal Code § 291 (damage to, destruction of or removal of all types of property). This kind of unclear implementation, however, did seemingly not equate to lack off or improper implementation[646] despite the lack of clarity that concerned the Commission.[647] It should be noted, however, that at the time the Commission did not have any power to bring action against Denmark for failing to implement the Framework Decision correctly, since the Framework Decision was adopted under the third pillar, under which the Commission had limited powers.

The Commission's report on the implementation of the Framework Decision concluded that in view of the emergence of botnets and massive simultaneous attacks against information systems (presumably, DDoS, or distributed denial of service) the Commission was going to aim at finding legislative responses to those threats.

7.2 The 2013 Directive

That response came in 2010 in the form of a proposal for a directive on attacks against information systems, which would amend and repeal the 2005 Framework Decision[648] with respect for the countries participating.[649] Apart from the new focus on botnets and massive simultaneous attacks, the directive proposal also directed its attention to "tools", naming malware and botnets as

[646] COM(2008) 448 final, pp. 5-6
[647] Granted, from the wording of the Danish criminal code § 291 alone, it is not apparent that it necessarily has anything to do with hacking or non-physical damage, such as the impairment of data integrity.
[648] COM(2010) 517 final
[649] The UK, Ireland and Denmark opted not to participate. See the directive's preamble recitals 31, 32 and 34.

examples.[650] The Directive, like its predecessor the 2005 Framework Decision, again builds on the Council of Europe's Convention on Cybercrime.[651]

The illegal access prohibition changed when the Directive was adopted. The offense is now provided for in article 3 of the Directive, and reads as follows:

"Member States shall take the necessary measures to ensure that, when committed intentionally, the access without right, to the whole or any part of an information system, is punishable as a criminal offence where committed by infringing a security measures, at least for cases which are not minor."

The wording, albeit still staying close to that of article 2 of the Convention on Cybercrime, now requires the additional element that a security measure must have been infringed. The criminalization of minor cases appears to remain optional, given the language "at least for cases which are not minor" indicating that every case of illegal access that is not minor must be criminalized and punishable.

At this point, one might ask why the Convention was not updated to respond to DDoS and botnet threats, as it was already being ratified by a number of countries. The Commission briefly addressed this option, as an alternative to EU legislative action, both in the proposal and in its impact assessment.[652] The Commission argued that it would require substantial renegotiation of the Convention, a process, which would take a long time, and considering that the proposal includes introduction of aggravating circumstances and penalties (increased) on which no agreement could be reached during the negotiations of the Convention. The Commission then concluded that there is no international willingness to renegotiate the Convention, as renegotiation would interfere with the ratification process, which is still underway.[653]

The Commission again defined how it interpreted "minor cases". "Minor cases" was introduced as an element of flexibility and the intention was to allow Member States not to cover cases that in theory fit the definition of the crime but where the protected legal interest is not harmed, for example, acts committed by young people attempting to prove their expertise with computers.[654] This makes it rather clear that minor cases are cases where every single element of the offense, including infringing security measures, is present; adding to or detracting elements from the offense as it is defined in article is not allowed for the purposes of excluding (by adding elements) or including (by detracting elements) minor cases. This indicates at least that the Commission is of the opinion that even where security measures are infringed (an ostensibly narrower scope of "illegal

[650] COM(2010) 517 final, p. 3
[651] Dir. 2013/40 EU, preamble recital 15
[652] SEC(2010) 1122 final, p. 26
[653] SEC(2010) 1122 final, p. 26
[654] COM(2010) 517 final, p. 7-8

access" than required under the Framework Decision), a case could be minor in the sense that the protected legal interest was not harmed.

On August 14 2013, Directive 2013/40/EU on attacks against information systems amended and replaced the Framework Decision. Some differences between the Directive and the old Framework Decision appear, on which the proposal for the directive and the impact assessment do not seem to explain. At least six of these differences are of immediate interest.

First, in the Directive's preamble, recital 12, it is acknowledged that identifying and reporting threats and risks, and vulnerabilities of information systems are germane elements of prevention of and response to attacks, as well as to improving the security of information systems. The recital encourages Member States to provide ways of legal detection and reporting of vulnerabilities. Since the meaning of this recital is not discussed directly in the preparatory works, it is hard to understand what it entails, other than, of course, that it is not binding on Member States, since it is placed in the preamble. The question is whether such legal detection and reporting of vulnerabilities would also cover security researchers/hackers that are not affiliated with the person, legal or natural, whose system is vulnerable; or whether it simply means that security researchers with express consent from the system's owner are not committing a crime when fulfilling their contractual agreements of finding and reporting vulnerabilities. The above-discussed dispute between the drafters of the Convention on Cybercrime with respect scope of the Convention's article 2 appears to have been restated in the directive's preamble – to a certain extent – because although there seems to be at least some consensus as to the need to allow for some discovery of and reporting of vulnerabilities, no substantive provisions provide a concrete solution to the problem related to IT security researchers' discovery, reporting and disclosure of security vulnerabilities.

Second, the preamble's recital 17 states that in the context of the Directive, contractual obligations, terms of use, terms of service and labor disputes involving access to and use of the employer's systems for private purposes should not incur criminal liability where the access is deemed unauthorized solely on those bases. As will become apparent in the chapter on authorization with respect to insiders, this addition to the Directive's preamble is very important. The same limitation of scope is being proposed in the US due to the expansive interpretation of the CFAA.[655] In light of

[655] See proposed bill, Aaron's Law, introduced in 2013. It stalled in committee, but was reintroduced in 2015. See coverage on e.g. the Electronic Frontier Foundation's website at https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself. Last visited on 26 August 2015.

the development in US case law (regardless of whether that development was considered or not), i.e. the rather intense circuit split discussed later in this dissertation, and the ongoing attempt to amend the American Computer Fraud and Abuse Act to definitively exclude these as bases for criminal liability[656], it makes perfect sense to exclude these acts from the scope of the Directive.[657] However appreciated this preamble recited is, there is no hint in the preparatory work as to why this recital suddenly appears.[658] The recital also states that the directive is without prejudice to the right of access to information, but that the directive may not at the same time serve as a justification for unlawful or arbitrary access to information. What arbitrary access to information entails is not explained, and therefore leaves one wondering.

Thirdly, as touched upon above, limiting illegal access to instances where a security measure has been infringed is *no longer optional*. This limitation is now a constituent element of article 3, which replaced the Framework Decision's article 2 prohibiting illegal access.

Fourth, illegal interception is now also criminalized in article 6 of the directive, which aligns the EU legislation even more with the Convention.

---

[656] See proposed bill, Aaron's Law. Available at Senator Ron Wyden's (D-Ore.) Senate webpage at https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-. Last visited on 26 August 2015.

[657] It is unknown whether the disagreement between US courts inspired this specific exclusion from the EU directive's scope, or whether there were already differing applications of domestic hacking provisions in the employer-employee context. Nothing in the directive's legislative history suggests such an internal split between domestic member state courts in this area. However, it is not entirely unlikely that some lessons were learned from the US, since the circuit split in the US at the very least provides a glimpse of a likely future involving internal disagreement between domestic member state courts and inconsistent application across the member states that will take years to litigate all the way to the Court of Justice for the European Union.

[658] The only hint at serious concerns about the scope of the Directive and the raising of penalties is found in what appears to be a Group Briefing from June 1012 by the Civil Liberties, Justice and Home Affairs (LIBE) Committee of the EU Parliament that found its way onto the Web. In the Briefing, LIBE maintains that "[t]he real problem is **weak IT security and systems resilience**, based on sloppy programming, on lack of redundancy due to cost cuts, and on a lack of incentives for systems manufacturers to change this, combined with **"as is" provisions in standard software licenses**. Discussions in LIBE have produced a wide consensus that it therefore is **not enough to focus on criminal law measures, and that the effect of those are negligible**." (p. 2) On page 3 of the briefing the group states that it nonetheless had achieved the adding of some safeguards, including that infringement of a security measure must be a required element of the offense, as well as violating terms of use or employment rules is not unauthorized access in a criminal sense. Furthermore, the group appears very concerned with "**protecting "white hat hackers" as integral part of the internet's immune system**" and states that the protection achieved in those terms were only a "very weak recital" in the preamble, and that the group had started a debate in the European Parliament regarding protection of those who find vulnerabilities. (p. 3) The document, which appears to be an internal working document and which does not appear to be available on e.g. the Parliament's legislative observatory, can, however, be found here https://s3.amazonaws.com/s3.documentcloud.org/documents/716937/attack-information-systems-group-briefing-june.pdf. Last accessed on 27 August 2015.

The fifth point of immediate interest is the criminalization in article 7 of hacker tools, or tools used for committing offences in article 3 to 6. Tools in this context are both computer programs, designed or adapted primarily for the purpose of committing the offences in article 3 to 6, and also computer passwords, access codes, or similar data used to access information systems when these are used to commit the aforementioned offences. Although criminalizing hacker tools is a response to remote access malware, botnets and the like, the article and the directive's preparatory works do not reveal much about how one would categorize tools that are dual-natured and are just as often used for legitimate purposes. The preamble's recital 16 at least recognizes the dual nature of these tools.

The sixth and final point of interest is the preamble's recital 26, which encourages Member States to take necessary measures to protect their critical infrastructure, and encouraging Member States to create measures incurring liability where legal persons have clearly not provided an appropriate level of protection against reasonably identifiable threats and vulnerabilities.[659] This preamble, although again not binding on Member States, in the very least indicates awareness that security derives primarily from actual security measures rather than the protection provided by criminal law. This is perhaps directly related to the binding text in article 3, where the infringement of security measures has become an obligatory element of the offense of illegal access. Perhaps the absence of protection of criminal law, some incentive is provided for those desiring that protection to implement actual security measures. This arguably introduces more certainty to the scope of illegal access provisions, but also raises the extremely important question of what a security measure is. This is discussed further below in the chapters on access and outsiders.

Furthermore, there is a noteworthy obstacle to harmonize of criminal law in the EU. Even though the Framework Decision and now the Directive mostly just replicate substantive criminal law provisions from the Convention, the Directive can perhaps achieve a bit more where the Convention cannot; a more uniform application in member states, with the support of the CJEU, insofar as the meaning of core elements forming the actus reus are not left to fall within the member states' margin of appreciation. Especially given the fact that general principles of criminal law are not harmonized, leaving further elements to member states' discretion, results in very limited "true"

[659] As an example of the necessity of such encouragement: The lackluster security of a Danish subsidiary of the American company CSC, which hosted many Danish government systems, was at the center of the biggest hacking case in recent Danish history.

harmonization. Attempting to harmonize criminal law where general principles of criminal law, such as intent, which can differ quite substantially between jurisdictions, is bound to be somewhat lackluster from the beginning because the extent of criminalization will be much greater in countries that e.g. consider dolus eventualis as a form of intent versus countries where dolus eventualis falls outside the realm of intent, falling instead within the realm of recklessness.[660]

Any differences there might be between member states' in terms of general principles of criminal law will arguably significantly compound the problems associated with further delegating to the member states the interpretation and construction of essential elements of the crime. Harmonization will indeed be minimal and perhaps not much more likely than under the Convention alone unless the CJEU gives core elements, such as "security measures" an authoritative construction. A question arises: If the directive will not achieve more than the Convention (and the Framework Decision and the directive mostly are copies of the Convention), is there truly a need for EU cybercrime law? That remains to be seen; especially where the Commission appears not to have comprehensively addressed the need for EU legislative action apart from the usual "cross-border" argument, which is regrettable seeing as criminalization ought to be the last resort rather than the first.[661] Although it is an interesting issue, whether or not there is a convincing justification for EU legislative action in terms of cybercrime falls outside the scope of this dissertation.

Directive 2013/40/EU repealed, replaced and amended the Framework Decision for those member states participating in the adoption of the directive. Denmark cannot adopt the Directive due to its reservations, and is still bound by the framework decision.[662]

---

[660] Sarah Summers: EU Criminal Law and the Regulation of Information and Communication Technology (2015), Bergen Journal of Criminal Law and Criminal Justice, Vol. 3, Issue 1, p. 58 (noting that, for example, dolus eventualis is a form of intent in Switzerland, whilst it would be categorized as recklessness in Scotland, leaving the scope of criminalization in Switzerland significantly broader than in Scotland.)

[661] Sarah Summers: EU Criminal Law and the Regulation of Information and Communication Technology (2015), Bergen Journal of Criminal Law and Criminal Justice, Vol. 3, Issue 1, p. 54 (pointing out that the case from criminalization was neglected, and thus questions relating to proportionality and necessity of criminalization that are essential to debating and understanding a resort to criminalization have not been properly addressed)

[662] See Directive 2013/40/EU, preamble recital 34 ("Since the amendments to be made are of substantial number and nature, Framework Decision 2005/222/JHA should, in the interests of clarity, be replaced in its entirety in relation to Member States participating in the adoption of this Directive"), as well as article 9 of Protocol no. 36 on transitional provisions ("The legal effects of the acts of the institutions, bodies, offices and agencies of the Union adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the Treaties. The same shall apply to agreements concluded between Member States on the basis of the Treaty on European Union."), and cf. article 2 of Protocol no. 22 ("acts of the Union in the field of police cooperation and judicial operation in criminal matters adopted before the entry

into force of the Treaty of Lisbon which are amended shall continue to be binding upon and applicable to Denmark unchanged.")

8 THE DANISH HACKING PROVISIONS

8.1 The Danish Criminal Code § 263 (2) and (3)

The Danish criminal code § 263(2) is popularly known as "the hacking provision". Subsection (3) increases the maximum sentence available where subsection (2) is violated under aggravating circumstances. The rationale of the hacking provision and its general purpose are explored in the next section. This section is simply reserved for citing the statutory text for future reference and as a starting point for the discussion below of the provision's legislative history.

Subsection 2: "Any person who unlawfully obtains access to another person's information or programmes designated for use in an information system shall be liable to a fine or to imprisonment for any term not exceeding one year and six months."[663]

Subsection 3: "Of the acts mentioned in Subsections (1) and (2) above are committed with the intent to procure or make oneself acquainted with information about trade secrets of a firm, or in other particularly aggravating circumstances, the penalty may be increased to imprisonment for any term not exceeding six years. This penalty also applies to the acts described in Subsection (2) above in the case of offences of a more systematic or organised nature."[664]

8.2 Legislative history of the Danish hacking provision

8.2.1 The 1985 amendment to the Criminal Code

In early 1984, the Danish Ministry of Justice requested that the Criminal Law Committee review the Criminal Code with a view to amending the law to ensure its applicability to computer crime. A year later, in early 1985, the Committee delivered its report to the Ministry of Justice.

The Committee recognized that computer crime legislation was an item on the agenda in many countries at the time, and noted that the vast bulk of existing research on variations in the methods

[663] Translation taken from Malene Frese Jensen, Vagn Greve, Gitte Høyer & Martin Spencer: The Principal Danish Criminal Acts (2006), p. 62. A caveat must be noted; the authors translated the word "uberettiget" as "unlawfully", where perhaps "without right" would be a more appropriate translation given that the term "unlawfully" more accurately corresponds to "ulovlig".

[664] Translation taken from Malene Frese Jensen, Vagn Greve, Gitte Høyer & Martin Spencer: The Principal Danish Criminal Acts (2006), p. 62.

used to commit computer crimes was taking place in the United States. Similarly, it was also noted that hacking statutes contained elements that were largely the same across many legal systems.[665]

At the very outset of the Committee's report the Committee emphasizes, like its American counterparts in Congress, that implementation and use of security measures undoubtedly has far greater preventative effect than a few amendments to the Criminal Code.[666]

Very early on in the report the Committee distinguishes between two sets of offenders by using the terms "employees" and "outsiders";[667] very similar to the usage of the terms "insiders" (employees are ostensibly always used as examples of "insiders") and "outsiders" in the US Committee reports on computer crime.[668]

The trespass provision (§ 264) was found insufficient with respect to computer crime, for example, because the trespass provision did not cover any actions carried out by the offender once he has entered a place without right (i.e. access information on computers at the location), nor did the provision cover insiders, such as employees, customers, etc.[669] And the privacy provision (§ 263) in effect at the time would have to rely on analogies or at least less clear extensive construction to cover computer crime.

In order to avoid applications by analogy and otherwise questionable constructions of existing provisions, the Committee opted for proposing a new subsection (2) in § 263.

Generally the chapter on privacy violations addresses various forms of access without right to places or information. The places and information covered are those that a person can reasonably expect to keep private.[670]

With respect to computers, the Committee explicitly stated that the new subsection would apply to both insiders who exceed their authorized access and outsiders who lack any and all authorization to use the computer.[671] The computer need not belong to someone else. The computer can very well belong to the offender. This is because the focus is not access to the computer as a thing, but on whether the information and programs accessed belong to someone else, such that use of one's own

[665] Criminal Law Committee Report, KBET 1985 no. 1032 at 15
[666] Criminal Law Committee Report, KBET 1985 no. 1032 at 17
[667] Criminal Law Committee Report, KBET 1985 no. 1032 at 17
[668] See section on the legislative history of the Computer Fraud and Abuse Act
[669] See Criminal Law Committee Report, KBET 1985 no. 1032 at 25
[670] Criminal Law Committee Report, KBET 1985 no. 1032 at 21
[671] Criminal Law Committee Report, KBET 1985 no. 1032 at 25

computer could incur criminal liability when one accesses information and programs belonging to others, but reside on one's own computer.[672] As an example, the Committee refers to the situation involving a leased computer. The lessor, just because he retains proprietary rights to the computer, does not for that reason have authorized access to the information belonging to the lessee during the time of the lease.

As will be explained later, the term "without right" encompasses more than just the "authorization" granted by the owner of the information or program. "Without right" (or "unlawful as Greve et al. translated "uberettiget") is also an indication that the legislature is aware of the breadth of the provision and that not every instance that fits the statutory language is necessarily within the legal scope of the provision. In explaining the warning inherent in the use of "without right", the Committee noted that questions of "right" were irrelevant with respect to outsiders (the impact of this statement is discussed later) and typical insider transgressions were those where an employee had e.g. used a password not belonging to him in order to gain access to information that are outside of his authorization. Sometimes the situation may be such that administrative sanctions are more appropriate than criminal punishment.[673] The view the Committee takes on outsiders

Unlike the American statute, the offender need not have obtained the information (even in the sense that the offender need just view the information). It suffices that the offender has managed to establish a connection to the content.[674]

If there was further intent to gain access without right to confidential information (trade secrets are mentioned in the statutory language whilst government systems are named as an example of aggravating circumstances in the report) a new subsection (3) provided for an enhancement for aggravating circumstances.

8.2.2 The 2002 amendment to the Criminal Code

In 2002, the Ministry of Justice assembled an ad hoc committee to review the law applying to modern technology. In particular, the Committee was assigned the task to review relevant legislation with a view to ratifying the Council of Europe's Convention on Cybercrime and prepare

[672] Criminal Law Committee Report, KBET 1985 no. 1032 at 26
[673] Criminal Law Committee Report, KBET 1985 no. 1032 at 26
[674] Criminal Law Committee Report, KBET 1985 no. 1032 at 26

for the implementation of the Framework Decision on attacks against information systems (EU law).

The 2002 Committee had the advantage that, unlike in 1985, the internet had now been commercialized, personal computers had found their way into a significant number of homes, and the Web had been invented. However, although the Committee describes the basic function of the Web and the possibility of new types of crime, the Committee did not address the extent of the scope of the illegal access provision to any great lengths nor the implications of the meaning of authorization, or right, with respect to publicly accessible systems on the Internet. In other words, what access without right means remained unclear.

Perhaps of relevance to the concept of authorization (or "right"), the Committee notes that implementation of security measures ought to be such that the protection provided for in criminal law should only be triggered where such security measures prove insufficient to prevent the offense.[675] In other words, the criminal law protection should be secondary to implemented security measures. Also the level of security measures in place are relevant in the sentencing phase. Such security measures should be in place not only for outsiders, but also for insiders, such as employees.[676] However, the Committee was aware of the possibility of unknown vulnerabilities in computer systems and that the owner of the system would not be able to prevent exploitation of such unknown vulnerabilities. Furthermore, a balance must reasonably be struck between security measure and practicality of using the system as well as the level of security having to be economically realistic. [677]

The 2002 amendment did not change much in the hacking provision. The term "data processing unit" was replaced with "information systems", and the maximum sentence was increased to reflect the vulnerability of the "IT-based society".[678]

[675] See Committee Report 2002 no. 1417 at 26
[676] See Committee Report 2002 no. 1417 at 26
[677] See Committee Report 2002 no. 1417 at 26
[678] Committee Report 2002 no. 1417 at 75-76

9 THE COMPUTER FRAUD AND ABUSE ACT

9.1 Current § 1030 statutes of interest

The Computer Fraud and Abuse Act contains quite a few provisions aimed at unauthorized access. Below, the ones most relevant to this dissertation are cited.[679]

U.S.C. 18 § 1030(a)(2)(C)

Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from a protected computer.

U.S.C. 18 § 1030(a)(4)

Whoever knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than § 5,000 in any 1-year period.

U.S.C. 18 § 1030(a)(5)(A)

Whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.

U.S.C. 18 § 1030(a)(5)(B)

Whoever intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage.

U.S.C. 18 § 1030(a)(5)(C)

Whoever intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage and loss.

U.S.C. 18 § 1030(e)(1) defines "computer"

[679] U.S.C. stands for United States Code. 18 refers to Title 18 of the United States Code. § 1030 can be found in Chapter 47 of Title 18.

The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

U.S.C. 18 § 1030(e)(6) defines "exceeds authorized access"

The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.

9.2 Legislative history § 1030 (The Computer Fraud and Abuse Act)

The CFAA's scope has been expanded rather dramatically due to a mixture of small, but significant changes to the CFAA's language as well as the courts' often broad, and sometimes rather creative, readings of the CFAA. Below are the highlights from the Committee Reports produced as a part of the legislative process that give some insight into the original purpose of the CFAA. The chapters on authorization with respect to insiders and outsiders then show how the CFAA has been applied in practice.

9.2.1 1984 Report: H.R. Rep. 98-894

In 1984 the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (CADCFAA) was passed into law.[680]

The House Committee on the Judiciary stated in its report regarding the proposal for the CADCFFA that it was very difficult to determine the "exact nature and extent of computer crime" whilst also noting that it was a substantial problem and the future potential was immense.[681]

[680] See also history of the 1984 Act in Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), pp. 24-25
[681] H.R. Rep. 98-894 at **3694

The 1984 act was fairly narrow in the sense that it only protected a limited set of confidential or classified information, and yet the language was too vague to be applied in practice.[682] Ostensibly only one person was ever indicted under the 1984 act[683] until the Computer Fraud and Abuse Act was passed in 1986, fixing the language to a certain extent.

9.2.2 1986 Report: S. Rep. 99-432

The Senate Committee noted that the advent of the personal computer had created a new type of criminal "who uses computers to steal, to defraud, and to abuse the property of others."[684] The Committee noted that computers and computer data constituted a property that was unprotected against crime.[685]

The Committee did not subscribe to the belief that criminal law would be the most effective way of combatting computer crime. Rather, it made it clear that "much computer crime can be prevented by those who are potential targets of such conduct", citing and strongly agreeing with the statements in an American Bar Association report that primary responsibility for prevention fell upon the industry and individuals rather than the government.[686]

The Committee envisaged a federal criminal law response in form of punishment as appropriate "for certain acts" and that it would serve to deter and "reinforce education and security improvement programs."[687] In 1986, it did not seem that the legislature was looking to pass a sweeping criminalization of all wrongdoing committed by use of a computer. In fact, the Committee explicitly rejected such a sweeping approach, preferring an approach limited to cases where there was a compelling federal interest.[688] The objection to a sweeping statute was thus arguably only a concern for intruding unnecessarily on the states' ability to legislate on computer crime, and not a concern with overcriminalization. The concern for overcriminalization with respect to the public in

[682] Christine D. Galbraith: Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites (2004), 63 Md. L. Rev. 320, 328. See also discussion on CFAA of 1986 in Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), pp. 25-26
[683] Christine D. Galbraith: Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites (2004), 63 Md. L. Rev. 320, 328
[684] S. Rep. 99-432 at **2480
[685] S. Rep. 99-432 at **2480
[686] S. Rep. 99-432 at **2480-2481
[687] S. Rep. 99-432 at **2481
[688] S. Rep. 99-432 at **2482

general was limited in 1986, since the bill before the Committee only applied to federal interest computers, a concept that was quite narrowly defined.

One of the proposed changes to the 1984 act, was that the scienter in the sections specifically protecting the computers of financial institutions and government computers was changed from "knowingly" to "intentionally" accessing without authorization or exceeding authorization and obtaining information from that type of protected computer. The reason for this change was the desire to exclude from the scope those persons who accidentally access someone else's files or data.[689] The Committee was concerned with "insiders" in this respect and in the process explains its perception of "exceeds authorized access". The Committee wrote in terms of precluding liability: "This is particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file or data that happens to be accessible from the same terminal."

Privacy was an important factor with respect to the subsection regarding financial institutions. "Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data."[690]

Specifically with regard to the subsection on government computers, the Committee wanted to be very clear that government employees who were authorized to access and use a computer would not face prosecution for acts that were technically wrong, but did not "rise to the level of criminal conduct."[691] The Committee needed to balance the concerns for authorized users against "the legitimate need to protect government computers against abuse by 'outsiders'."[692] The balance was struck by not making criminals of employees who exceeded their authorized access to computers in the same department as they worked in. The Committee envisaged an employee who "briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at."[693]The Committee added that "[t]his is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain data."[694] The Committee proposed administrative sanctions for such cases rather than criminal sanctions. Thus

[689] S. Rep. 99-432 at **2483
[690] S. Rep. 99-432 at **2484
[691] S. Rep. 99-432 at **2485
[692] S. Rep. 99-432 at **2485
[693] S. Rep. 99-432 at **2485
[694] S. Rep. 99-432 at **2485

"exceeding authorized access" was excluded from the provision prohibiting unauthorized access to government computers and thus precluded liability in "purely 'insider' cases"[695]. Only where an insider accesses other departments' computers, and is thus "directly analogous to an 'outsider'"[696] did that subsection apply to government employees or others with authorized access to any government computer. Generally, it was reserved for "outsiders".

Of great interest is the Committee's introduction of the language "exceeds authorized access" which replaced "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend".[697] The Committee contended that this was a simplification of the previous "cumbersome" language. Later in the report it is explained by Senators Leahy and Mathias that replacing the "purpose" oriented language "removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization."[698] Administrative sanctions should suffice. This was supposed to give prosecutors "a clear, workable rule, regardless of the intricacies of a particular agency's computer access policies: absent a fraudulent motive, an employee could not be prosecuted for simple 'trespass' into one of his agency's own computers."[699]

The Committee stays true to its use of the concepts insider and outsider, in that it states that (a)(5) (causing damages) is only applicable to "outsiders".[700]

9.2.3 1994 amendment

The 1994 amendment[701] included few changes to the CFAA, but at least one of them has arguably had rather dramatic effect on the subsequent construction of the CFAA.

---

[695] S. Rep. 99-432 at **2485 (this was partially, but not solely, a response to concerns about criminalizing acts of whistleblowers)
[696] S. Rep. 99-432 at **2486
[697] S. Rep. 99-432 at **2486
[698] S. Rep. 99-432 at **2494-2495
[699] S. Rep. 99-432 at **2495
[700] S. Rep. 99-432 at **2488
[701] See also brief rundown of the 1994 amendment in Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), pp. 26-27

§ 1030(a)(5) continues applying to outsiders, i.e. those lacking any authorization to access the computer, but now also applies to malicious insiders.[702] In this context, the Committee, in the 1996 Senate report whilst describing the 1994 amendments, specifically uses the words "integrity" and "availability"[703] of information with respect to the interests protected under subsection (a)(5) and cites other provisions with respect to protection of "confidentiality".[704] Subsection (a)(5)(A) would target anyone who intentionally damages a computer without authorization – insiders and outsiders alike. Subsection (a)(5)(B) would apply to outsiders who access the computer without authorization and recklessly cause damage. Subsection (a)(5)(C) would invoke misdemeanor penalties for outsiders who access the computer without authorization and cause damage (accidentally or negligently). That is, insiders would have to cause the damage intentionally, whereas outsiders would incur liability under (a)(5) by causing the damage intentionally, recklessly or simply just causing the damage without any scientier requirement attached.[705]

The 1994 amendment was the one that introduced the civil remedy. The civil remedy allows victims to state a claim in federal court where they can sue for compensatory damages, injunctive relief or other equitable relief.[706] The civil remedy is provided in § 1030(g). The statute of limitations for civil claims would be two years; lower than that for criminal prosecution. A sponsor of the amendment expressly stated that the intention was not to "open the floodgates to frivolous litigation".[707] Granted, before the 1996 amendment, the number of possible plaintiffs was limited because prior to 1996, the CFAA only applied to so-called "Federal interest computers".[708]

At present, a plaintiff can state a civil claim under the CFAA, if one of five[709] factors are present; where the offense caused loss to one or more persons during any 1-year period totaling at least $5,000 in value usually being the triggering factor for most civil claims.

---

[702] S. Rep. 104-357 at *9. The change appears to have occurred in the 1994 amendment, which will not be subject to specific discussion. See e.g. Orin Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota L. Rev. 1561, 1566

[703] The terms "integrity" and "availability" are even included in the statute's definition of "damage" which means "any impairment to the integrity or availability of data, a program, a system, or information". See 18 U.S.C. § 1030(e)(8).

[704] See generally discussion of § 1030(a)(5) in S. Rep. 104-357 at *10 et seq.

[705] S. Rep. 104-357 at *11

[706] S. Rep. 104-357 at *12

[707] Christine D. Galbraith: Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites (2004), 63 Md. L. Rev. 320, 329

[708] See discussion in Christine D. Galbraith: Access Denied Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites (2004), 63 Md. L. Rev. 320, 329 et seq.

[709] § 1030(g), cf. § 1030(c)(4)(A)(i)(I-V)

9.2.4 1996 Report: S. Rep. 104-357

In stating the purpose of the 1996 amendment[710] to the CFAA the Committee stated that the amendment would strengthen the CFAA "by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks."[711] The IT security language, i.e. confidentiality, integrity and availability, and the mentioning of privacy (which arguably is a specific concern relating to confidentiality of information), is rife within the 1996 Committee report. The insider/outsider distinction also persists from earlier reports.

Until the 1996 amendment, the CFAA had protected only unauthorized access to the types of computers that held classified or private financial record information. The Committee focused on gaps in coverage with respect to privacy protection. Namely, that the confidential and classified information was not protected from government employees "who abuse their computer access privileges to obtain Government information that may be sensitive and confidential."[712]

§ 1030(a)(2) was amended to increase the protection of privacy and confidentiality of information on computers.[713] It furthermore extended the coverage to "computers used in interstate or foreign commerce or communications, if the conduct involved an interstate or foreign communication."[714]

According to the Committee, the purpose of (a)(2)(C) is to protect against "interstate or foreign theft of information by computer."[715] At the center of (a)(2)(C) is "the abuse of a computer to obtain information." [716] That is, (a)(2)(C) targets breaches in confidentiality of information. The seriousness of the breach is primarily reflected in the value of the information and the intended future use of the information.[717] However, it is of note that the future use and the value does not in itself make the access unauthorized, and as such, should only affect sentencing – not determination of guilt. The Committee took the seriousness of the breach into account when evaluating the severity of the punishment.[718]

---

[710] Amended through adoption of the Economic Espionage Act of 1996. See also an account of the changes made through that amendment in Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), pp. 27-28
[711] S. Rep. 104-357 at *3
[712] S. Rep. 104-357 at *4
[713] S. Rep. 104-357 at *7
[714] S. Rep. 104-357 at *7
[715] S. Rep. 104-357 at *7
[716] S. Rep. 104-357 at *7-8
[717] S. Rep. 104-357 at *8
[718] See generally S. Rep. 104-357 at *8

When discussing the exception for "computer use", i.e. use of computer time, in subsection (a)(4) (on computer fraud) the Committee averred that the blanket exception was too broad , and for example, hackers had gained access to supercomputers for the purposes of running password cracking programs.[719] However, the Committee's inquiry into *purpose* for use of the computer in this instance is irrelevant in with respect to determination of guilt. The hackers had already gained access without authorization (since they lacked any and all authorization to access the computer); their purpose for doing so is irrelevant with respect to guilt. The reason the Committee is discussing *purpose* for hacking into a computer is in the context of revoking a blanket exception for stolen computer time the value of which could vastly exceed the $5,000 value requirement under subsection (a)(4). The *purpose* discussion does not relate to whether hacking into the supercomputer was unauthorized or not, just whether the use of time should be counted towards the value required to apply subsection (a)(4), a felony, rather than the being a violation of e.g. (a)(2)(C), a misdemeanor.

One of the arguably most expansive amendments to the CFAA was replacing the term "Federal interest computer" with the term "protected computer". The new term, "protected computer" expanded the statute's scope to include all computers "used in interstate or foreign commerce or communications".

9.2.5 2001 and 2008 amendments

The 2001 and 2008 amendments[720] both substantially expanded the scope in a more or less discreet way. In 2001 the USA PATRIOT Act expanded the definition of "protected" computer to also covering computers located in foreign countries where the computer affects interstate or foreign commerce or communications.[721] Additionally, the 2001 amendment adjusted the CFAA by explicitly excluding product liability claims – which appears to be the only case of Congress reacting to a very broad construction of the CFAA[722]; a Texas federal judge had construed the

[719] S. Rep. 104-357 at *9
[720] See also overview in Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), pp. 28-32
[721] Orin Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota L. Rev. 1561, 1568
[722] It is curious that Congress has only reacted to perceived overcriminalization, and did so rather swiftly, where it has been to the detriment of the tech industry, but has seemingly remained silent and dormant despite numerous cases that have attract sharp criticisms of broad constructions to the detriment of (typically) individuals, as well as calls for

statute quite creatively to allow such claims under the CFAA, generating .[723] In 2008, the Identity Theft Enforcement and Restitution Act removed the requirement of interstate communication from § 1030(a)(2) meaning that under subsection (a)(2)(C) "*any* unauthorized access to *any* protected computer that retrieves *any* information of *any* kind, interstate or intrastate, is punishable by the statute."[724] Furthermore, the definition of "protected computer" was again expanded by adding the language "or affecting" in terms of a computer's relationship with interstate or foreign commerce or communication. As explained by Orin Kerr, "affecting interstate commerce" is what he calls "a term of art" that means that Congress intended to push the Commerce Clause to its limits, in that this language allows Congress to regulate purely local issues normally regulated by the states. Thus, the 2008 amendment expanded the CFAA from applying "only" to all computers connected to the internet, to applying to all computers everywhere in the world, inside and outside the United States.[725]

---

reforms by interest organizations such as the Electronic Frontier Foundation and others. See more on the broad construction of the CFAA in the chapters on authorization with respect to insiders and outsiders.

[723] A case out of a federal district court in Texas had read product liability into the statute. See *Shaw v. Toshiba*, 91 F.Supp.2d 942 (E.D. Texas 2000). As mentioned in the note above, Congress acted with surprising haste, making it clear in 2001, only a year after Shaw v. Toshiba, that product liability was excluded from the scope of the CFAA.

[724] Orin Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota L. Rev. 1561, 1569

[725] Orin Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota L. Rev. 1561, 1570-1571

10 ACCESS

The basic hacking provisions typically contain three elements: "without authorization", "access" and "computers" (and/or "information" and "programs") in order to prevent so-called hacking, and all of these elements have the potential to be applied very broadly, although "without authorization", as will be shown, is the most ambiguous and leaves incredible room for creativity.

Given that legislatures, such as the US and the Danish legislature, had a comparative eye on traditional trespass and other property-based law, it is not that odd that concepts such as authorization and access, followed by reference to the object in which there is a property interest, form the core of hacking statutes. However, with respect to computers, it is not so clear-cut when one has accessed a computer and information when compared to entering a building or other property. There are a few ways of perceiving access. In this chapter the problem related to construing "access" is first briefly introduced below by showing alternative ways of construing access. Then, in the following sections, it will be explored for which alternative, if any specific one, there is support in the legislative history and in case law of the various hacking provisions. Furthermore, a section is dedicated to showing the difference between "access" and "use" in terms of information, a distinction that has been made by many US courts to separate plaintiff claims of unauthorized access to information from claims ultimately do not relate to the act of "access" itself, but rather relates to subsequent unwanted "uses" of information that the defendant had authorization to access.

10.1 Different perspectives on "access"

I briefly introduced the system theory concepts used by Orin Kerr (and, to an extent, Mads Bryde Andersen) in the chapter on problems with description. Advocating a broad construction of "access", Orin Kerr presents the concept of access from the external and the internal perspective.[726] From an internal perspective (which Kerr also referred to as the "virtual reality perspective") we view the computer as the physical object it is that one would need to get "inside" in order to have "accessed" the computer. Thus, from the internal perspective, access would not have taken place if someone opens a password protected file and is then confronted with a password prompt – akin to

[726] Also discussed briefly in Jonathan Clough: Principles of Cybercrime (2010), pp. 59-60

facing a locked door – but does not try to enter or get past the password prompt.[727] For the file to have been accessed, the file needs to be opened for the interaction with the file to constitute "access". Similarly, as seen from the internal perspective, accessing a public website would be perceived as "viewing a shop window from a public street".[728] That is, the internal perspective is concerned with how the users perceive or interpret the visualization of the code (often by way of analogies to things and processes we have experienced in the physical world), how they experience the code of e.g. a website as they use the website.

The external perspective is the perspective of the observer who is not himself a participant in the system. E.g. one observes the Internet as millions of interconnected computers, rather than how a user of the Internet may describe his experience of the Internet as a virtual reality. Thus, from the external perspective, any action that causes a computer to function[729] constitutes access ("any successful interaction with a computer"[730]).[731] That is, sending an email constitutes access to every single computer through which the email is routed as well as access to the computer that is the emails final destination.[732] For example, if you use Google's email services – even if you never use Gmail's web interface to send an email but rather you send emails through an email client on your computer – you are accessing Google's computers every time you send an email, as well as accessing every other computer the email is routed through subsequently, including the destination computer. Sending a "ping" to another computer, causes the computer to respond by confirming its existence, and thus, form an external perspective constitutes accessing a computer. Similarly, this applies with respect to provisions prohibiting unauthorized access to information because the

---

[727] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1619-1620

[728] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1620

[729] The UK provision seems to accept something akin to this approach but with a distinct addition that distinguishes it from the approach preferred by Kerr. The UK provision prohibits "causing a computer to perform any function with intent to secure or enable access". The addition of "with intent to secure or enable access" distinguishes "causing to function" from "access". However, how this has been construed in practice is beyond the scope of this dissertation. See Jonathan Clough: Principles of Cybercrime (2010), p. 62. Clough notes that the UK approach "is extremely broad as there is no limitation on the manner in which the defendant causes the computer to perform any function. Simply switching a computer on, or attempting to enter a password would both be encompassed by the terms of the section." Jonathan Clough: Principles of Cybercrime (2010), p. 63

[730] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1647

[731] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1620

[732] See Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1621

information yielded from a ping can be viewed as accessing information.[733] Under the Danish hacking provision, which prohibits unauthorized access to information and programs, sending an email through the Gmail service could constitute accessing a program belonging to another. That there are different ways of perceiving facts means that a choice must be made with respect to which perspective is the "applicable perspective" in a case. That choice will then affect the legal outcome of the case, because the legal rule is applied to facts as seen from the chosen perspective. For example, when considering whether someone has violated a hacking statute, should sending an email be considered "access" to every single computer that the email is routed through on its way across the Internet, or should sending an email not be considered "access" under a hacking statute?

Orin Kerr argues that the broad construing of "access" – the external perspective – is the most logical choice, because the internal perspective yields arbitrary results as to whether a transmission to a computer, or interaction with a computer, constitutes access. For example, under the internal perspective accessing a public website would not qualify as access even though files were retrieved from the web server so that the website could be displayed on the user's computer – because under the internal perspective the public website, e.g. Amazon's website, is viewed as a shop window as seen from a public street. However, as noted by Jonathan Clough (who generally favors the broad reading proposed by Kerr), under Kerr's external perspective "access becomes synonymous with use in its broad sense"[734] and that the broad reading would leave little if any room for conduct that constitutes "attempt to access".[735] Rather than opting for a narrow reading of access that conflicts with the technical reality (because retrieving a website from a server requires the user to establish a connection to the server, regardless of whether it "feels" like window-shopping) and that the narrow reading thus calls for judges to make arbitrary distinctions between what constitutes access and what does not, Orin Kerr argues instead that "authorization", rather than "access", should be construed narrowly to limit the scope of unauthorized access statutes.[736]

---

[733] From the external perspective "we see that access to a computer necessarily involves access to data." Jonathan Clough: Principles of Cybercrime (2010), p. 59

[734] Jonathan Clough: Principles of Cybercrime (2010), p. 69 ("use in its broad sense" refers to "any interaction with the computer by way of inputs is a 'use' of that computer". Clough, p. 68)

[735] Jonathan Clough: Principles of Cybercrime (2010), p. 70

[736] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1648

Another commentator, Patricia Bellia,[737] conversely, argues in favor of a narrow construction of access. Bellia compares the broad reading ("transmitting electronic signals to a computer that the computer processes in some way"[738]) and the narrow reading ("conduct by which one is in a position to obtain privileges or information not available to the general public"[739]). She argues that adopting the broad reading of "access" opens hacking statutes up to contractual limitations on uses of a system and that violating such limitations would then trigger the application of unauthorized access statutes.[740] Bella argues that the more natural reading of "access" is rooted in a code-based approach; only circumvention of code-based protection of the system would constitute "access".[741] Under Bellia's theory, then "exceeds authorized access" in the US federal hacking statute could conceivably allow policy and contractual terms should be relevant in that respect.[742] [743] Bellia's point is, it appears, that publicly accessible information should be excluded from the scope of that which can be "accessed" in the legal sense that the word "access" is used in hacking statutes. Her argument has its appeal, because the policy issue she addresses (information that is publicly accessible, such as websites) has gone unaddressed by the legislature in terms of whether access to such information falls within the scope of hacking statutes or not. I will discuss hers and Orin's point in more detail in the below section on "access" in US law. However, now I will examine which approach – if any – the Convention on Cybercrime supports, as well as which approach – if any – is supported by the EU, Danish and US legislatures based on legislative history and the statutory text, and which approach has been adopted by the courts.

10.2 The Convention on Cybercrime

The Convention's article 2, which prohibits the intentional "access to the whole or any part of a computer system without right" does not define "access"; nor does the Convention's article 1, which does, however, provide definitions of other concepts used in the Convention, such as "computer system" and "computer data".

---

[737] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, pp. 2164-2273
[738] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2253
[739] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2254
[740] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2254
[741] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2254
[742] Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2254
[743] In other words, the inclusion of contractual and policy violations under the CFAA, which Bellia argues is undesirably included through a broader reading of "access", she then ostensibly accepts it under the reading of "exceeds authorization", and thus accepts contracts as a basis for limitation of authorization.

The Explanatory Report provides an explanation, to an extent, of what is meant by "access" in the Convention's article 2:

""Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. "Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter." [744]

[744] The Explanatory Report para. 46

- *Hardware*
- *Components*
- *Stored data of the system installed*
- *Directories*
- *Traffic data*
- *Content-related data*

The Explanatory Report's description of what *access* comprises provides an outer limit; namely that the mere sending of an email message or file to the system does not constitute access. In other words, the Convention's Explanatory Report appears to support what Orin Kerr calls the internal perspective in the sense that the computer system, or any part of it, must be entered into; indicating something more must be done than simply causing a computer to function. However, the above listed parts of the computer system cited by the Report, leave some uncertainty with respect to whether e.g. simply playing with a keyboard when the computer is turned off constitutes access to/entering of "any part of a computer system". Since article 2 is meant to protect against attacks on confidentiality, it not very plausible that simply fiddling with a keyboard where doing so cannot compromise confidentiality, because e.g. the computer is turned off or the keyboard is not connected to a computer, will lead to a criminal conviction, however, the plain language of the article requires construction to reach such a result, since it does not follow directly from the article's language as such.

Article 2 of the Convention prohibits the unauthorized access to the whole or part of a *computer system*; the computer system being defined in article 1 as "any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [.]" As recalled, the Danish provision prohibits the unauthorized access to *information and programs* rather than *systems* or *computers*. The question is whether the language in the Convention's article 2, referring to *systems*, has any legal consequences regarding e.g. whether someone who already has authorized access to the system, but maybe not all of it, can violate such an "unauthorized access" statute? It is doubtful that article 2 could reach any acts committed by someone who had general authorization to use the system, but perhaps was unauthorized to access certain databases on that system, had it not been for the fact that the Explanatory Report defines "any part of a computer system" as including stored data on the system. In absence of words along the lines of "exceeding authorized access", the initial authorized access to the computer system would be the only access authorization that mattered – not the subsequent unauthorized access to specific information contained on that computer; a computer to which the access was, after all,

authorized.[745] That is, any access to information on a computer subsequent to the initial authorized access to that *computer* would necessarily be authorized as well – at least under a hacking provision forbidding unauthorized access to a *computer* in absence of the addition of the concept "exceeds authorized access" or "any part of a computer system".

In terms of the Convention, article 2 is thus capable of reaching both those who have no authorization to use the computer and thus no authorization to access any information on it, as well as those who have authorization to use the computer and access some information on it, but are unauthorized to access certain other information on the computer. The inquiry into whether access is authorized would be relevant not only with respect to the computer as a whole, but also whether access to specific information was authorized. However, the Explanatory Report appears to limits the meaning of "access" to something akin to the internal perspective by rejecting that sending emails constitutes "access". "Accesses" to computers through which packets are routed in the course of connecting to another computer over the internet would likely similarly be excluded from the scope.

10.3 The EU Framework Decision and EU Directive

Neither the Framework Decision nor the Directive define "access". Furthermore, the Commission's reports preceding the adoption of both the Framework Decision and the Directive leave the term undefined and undiscussed. Perhaps one may assume that the definition of access follows that of the Convention's Explanatory Report, since both the Framework Decision and the Directive are based on the Convention and largely mirror the substantive articles therein. There is, however, no concrete evidence for or against such a presumption being made by the Commission with respect to whether definitions provided in the Explanatory Report are carried over into the interpretation of either the Framework Decision or the Directive.

It is uncertain whether the Framework Decision is based on the broad or narrow reading of access, but a narrower approach may be likely given the intended alignment with the Convention on Cybercrime.

[745] See also Jonathan Clough: The Principles of Cybercrime (2010), p. 92

The Directive makes the distinction, and thus also the choice, between broad and narrow readings of "access" largely irrelevant, since infringement of security measures is a mandatory element of illegal access offenses. The directive seemingly draws the line of relevant access at the system's security perimeter; the directive, however, does not specify whether the security measure needs to be a technical/logical one as opposed to physical security, and what form such security could hypothetically take. This new element effectively excludes, largely but not entirely, from the scope of "illegal access" acts such as portscanning (which could trigger liability under a broad construction of "access" if authorization is absent), access to publicly accessible websites where such access is unauthorized due to contractual obligations, as well as other acts that exist in the penumbra of broader illegal access provisions. Essentially though, the limiting effect of restricting illegal access provisions to those cases that involve infringement of security measures, hinges entirely on what is meant by "security measures". A naïve user might for example think that not linking to a webpage on his webserver (a form of "security through obscurity") means that the absence of that link constitutes a security measure or he may think the webserver is "undiscoverable" because he has told no one about it (not that subjective perceptions of what is a security measures should ever determine what does and does not trigger criminal liability). What is meant by "security measure" in the context of directive, such that a circumvention of the security measure triggers criminal liability under the relevant implementing national provision, is regrettably unclear.[746] This is an important question that concerns the standard of security that a company, for example, must live up to in order to obtain protection under criminal law, as well as signaling to those regulated by the law whether e.g. symbolic "security measures", for example those that rely on "security through obscurity" in form of simply not sharing the location of a website, constitute security measures in the context of the directive. Similarly, there is the question whether certain people can be selectively excluded from visiting public websites, e.g. by blocking their IP-address, and their circumvention of that block thereby triggers application of illegal access provisions.

[746] See also P. Freitas and N. Gonçalves: Illegal access to information systems and the Directive 2013/40/EU (2015), International Review of Law, Computers & Technology, Vol. 29, No. 1, p. 60 (The authors appear to consider only that which is or may be lost by restricting the scope of the illegal access article, failing to consider or recognize the incredible and problematic breadth the scope was capable of having prior to restricting the scope to only those cases where security measures had been circumvented. As will become apparent in the chapters on authorization in this dissertation, particularly the sections on US law, "security measures" in itself is a concept requiring definition because the concept is capable of great breadth and arbitrary distinctions not only in cases where criminal liability ought to be incurred but is not, but also in cases where criminal liability is incurred but arguably should not have been incurred. The concept thus brings with it both over- and undercriminalization; however, the authors of the abovementioned article focus only on the latter and thus provide no alternative solution to restricting the scope.)

Although the requirement of infringement of security measures excludes the most problematic of the possible readings of broader illegal access provisions, it raises a new question, albeit perhaps a narrower one: What is a security measure?

10.4 Danish law

The Danish criminal code § 263(2) prohibiting unauthorized access reads as follows:

Subsection 2: "Any person who unlawfully obtains access to another person's information or programmes designated for use in an information system shall be liable to a fine or to imprisonment for any term not exceeding one year and six months."[747] [748]

The provision defines neither "without right" (or unlawfully, as Greve et al. translated it) nor "access", nor does it contain any additional requirements[749], like intent to defraud or infringement of security measures, to limit the scope of the provision. The concepts are not defined anywhere else in the criminal code either. Thus, the concept of "access", in and of itself, does not establish any critical limit to the scope. The provision does not allude to what access is and when something constitutes access. Is any interaction sufficient, such as pinging a computer, for the simple reason that "some" information is obtained in the form of knowledge that the computer exists at a certain IP address?

As far as § 263(2) goes, the Committee who drafted the provision, observed the novel context in which the rule would apply and therefore may have given consideration to the meaning of access in the context of computers.

[747] Translation taken from Malene Frese Jensen, Vagn Greve, Gitte Høyer & Martin Spencer: The Principal Danish Criminal Acts (2006), p. 62. A caveat must be noted; the authors translated the word "uberettiget" as "unlawfully", where perhaps "without right" would be a more appropriate translation given that the term "unlawfully" more accurately corresponds to "ulovlig".

[748] Comparisons will be drawn to the broadest provision of American Computer Fraud and Abuse Act 18 USC § 1030 (a)(2)(C) (Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer shall be punished as provided in subsection (c) of this section.).

[749] Note that in the Danish criminal code, intent is the mens rea required unless negligence is specifically mentioned in the provision; see the Danish criminal code section 19.

§ 263(2) was passed into law in 1985. Its raison d'être was, and still is, to cover unauthorized access to information and programs intended to be used in an information system, to which the older § 263(1) was only tentatively applicable.[750]

Committee report 1985 no. 1032 reveals a few things about the legislative intent, or at least what the legislator may have understood by "access". First of all, the report leads with a short and superficial description of how networks and computers work from a technological point of view, which could, however tentatively, indicate a preference for a broad reading of access. In terms of providing clues to how the term "access" should be interpreted the report provides only a short, vague description as part of a summary of how to interpret § 263(2):

"[…] [T]he person in question, by connecting to and operating the computer, shall have succeeded in connecting to its contents, while conversely it is not required proven that he has gained knowledge of anything. It is not of any great importance to lay down a precise boundary between attempt and completed crime. Situations where a person with the intent to obtain information, but who is unfamiliar with the password, during his operating of the system manages only to determine that a screen display shows an access restriction to the system's content, must be counted as criminal attempt. On the other hand, it is a completed offense that the person in question has gained access to other information than that in which he is interested."[751]

This explanation appears to militate in favor of the narrow reading of access, because the reference to a success in connecting to contents on the computer. However, that just raises the question of what the Committee understood by "content". Is information from a portscan "content"? If yes, then the Committee's explanation supports a broad reading of access. However, what to provide strong support for a narrow reading, is the Committee's view that viewing a password prompt constitutes attempted unauthorized access rather than a completed offense (insofar as the offender actually intended to obtain information protected by the access restrictions).

Although the quote from the 1985 Committee report largely seems to suggest a narrow interpretation of "access", the ostensible narrow approach could also hinge on what a court deems to be "content" (presumably, information and programs, which are the intangible material protected by § 263(2)). Two Danish district courts indicate that portscanning is not covered by the scope of § 263(2), unless the portscan is a preparatory act carried out by a defendant who has the intent to gain

[750] Subsection 1 prohibits three acts, one of which is the accessing of archives, compartments and the likes without right (perhaps in some ways comparable to 'chattels'). For example opening desk drawers or boxes without right.
[751] Committee report 1985 no. 1032, 26-27. Quoted text translated from Danish to English by the author.

unauthorized access to the computer.[752] These constructions of "access" are more in line with the narrower reading, requiring the "entering into" a computer, rather than the broader "causing a computer to function", as well as being in line with the statement in the Committee report that simply viewing a password prompt is only an offense if there is intent to obtain information from the computer (indicating that the password prompt itself does not constitute information in that sense).

However, § 263(2) lacks a limitation on its scope, which the American CFAA, EU Framework Decision, EU Directive and the Convention do not. The Danish statutory language does not require that the information or the program actually reside on a computer when it is accessed. More specifically, information or a program can theoretically be "accessed" in the strict meaning of statutory language of § 263(2) where the information or program, existing only on regular paper, is *intended* for later use on a computer, but has not yet been so used at the time it is "accessed". In other words, the statutory language does not in itself require that the information or program "accessed" actually resides on a computer[753] and could strictly speaking be a piece of paper lying on a desk in an office building. Furthermore, the statutory language does not itself reasonably support a narrower reading that requires the information or program to reside on a computer.[754]

However, the language in the Committee's report and the comments on the bill provided by the Ministry of Justice, overwhelmingly suggests that a closer connection between the information or program and the computer is required. This is because both texts exclusively refer to use of a computer in order to access information or programs; i.e. that the information or program resides on a computer or its peripherals – not for example on paper for later use on a computer.[755]

Should the courts decide to give § 263(2) its "ordinary meaning" and thus depart from the implied presumption in the legislative history that the information or program resides on a computer, by construing the provision to include e.g. information on paper that is intended for later use on a computer, § 263(2) would at least match, if not greatly surpass, the reach of the unconstitutional

[752] According to an article on the website of the law firm Bird & Bird, at least two Danish courts have decided cases on portscanning; both courts seemingly considered that the portscanning itself did not constitute "access", but rather constituted an attempt to access where the defendant had intent to gain access, and the portscanning was a preparatory act. Portscanning for the sake of curiosity did not trigger criminal liability. See article on cases at http://www.bvhd.dk/videnbase/?task=show&uid=644&target=&category=19&cHash=d12682fb9c. Last visited 18 June 2015. The author has not had access to the two district court decisions.
[753] This oddity has been pointed out by Greve in Vagn Greve: edb-strafferet (1986), pp. 46-47
[754] See also Vagn Greve: edb-strafferet (1986), p. 46-47
[755] See also Vagn Greve: edb-strafferet (1986), p. 47

definition of "access" (i.e. approaching a computer) in the Kansas state computer crime statute that was deemed void for vagueness by the Kansas Supreme Court in *State v. Allen*. Such an expansive reading of § 263(2) arguably exceeds the Kansas statute's reach because § 263(2) does not require that the information is observed, altered, damaged or obtained by the offender; it merely requires that "access" has been gained to the information. Thus, a literal reading of § 263(2) would essentially mirror the Kansas computer crime statute's "approach a computer" definition of "access", albeit in relation to information in physical format. Construing "access" in that manner would likely violate article 7 ECHR, which prohibits both retroactive criminalization by the legislature and expansive judicial statutory constructions that are not reasonably foreseeable.[756] Approaching a piece of paper knowing or believing it contains information could theoretically trigger criminal liability if the information on the paper is meant to be used later on a computer. However, it is unlikely that Danish courts would construe § 263(2) that broadly.

10.5 US law

The Computer Fraud and Abuse Act does not define access, either. There is nothing in the legislative history that definitively points one way or the other in terms of whether the legislature supported a narrow or broad reading of access. The Committee reports for example are sufficiently vague so that one could find support for whatever approach one prefers; the same applying to the interpretation of authorization.[757]

In favor of a narrower approach to construing "access" is that it is arguably the approach most consistent with the general purpose of the CFAA. The CFAA started out with a fairly narrow scope; not in the sense that "authorization" and "access" were somehow clearer concepts, but because the act, in 1986 (and its 1984 predecessor as well), only protected certain very specific types of confidential and/or classified information residing on federal interest computers against unauthorized access. Specifically subsection (a)(2), the broadest subsection today, was supposed to

[756] See section on article 7 ECHR in the chapter on nullum crimen sine lege.
[757] Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819, 829-830. See also Warren Thomas: Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act (2010), Georgia State University Law Review, Vol. 27, Issue 2, Article 14. Available at http://readingroom.law.gsu.edu/gsulr/vol27/iss2/14.

safeguard privacy.[758] Because (a)(2) guarded privacy, the Committee emphasized that for that reason the term "obtaining information" included merely observing the data. The prosecution would not be required to show actual moving of the data to show that information had been obtained.[759] Furthermore, until 1996 the act focused only on Federal interest computers; not computers in general. In the later 1996 report, the Committee makes many references to the terms "confidentiality", "integrity" and "availability"; that is, computer security concepts used in the context of a report on a computer-related statute. In other words, such terms tend to indicate the existence of a security perimeter, since nothing that is accessible to the public is "confidential". Thus, in that sense, surely crossing a perimeter of some kind in the sense that a computer is entered and information obtained that is not publicly available.

The other side of the coin is that the CFAA, like most hacking statutes, is also based on the traditional idea of trespass. "Computer trespass" invokes concepts like "property" and "right to exclude". Thus, an owner exercises proprietary control over the computer and can choose who he lets interact with the computer. Such a concept, although arguably less problematic in 1986 where most computers were not reachable by every other computer by virtue of the Internet, is somewhat at odds with the state of things in the internet age. Delineating the perimeter of land property, which is necessarily connected to the rest of the world and cannot be "disconnected" from the world, is much easier and more obvious than trying to artificially draw a contrived line with respect to a "cyberproperty" that the owner, through his own volition, decided to make publicly accessible. If for example a computer running webserver software is connected to the internet, its existence will be discovered by other computers – likely within seconds.[760] Since scanning an IP address necessarily means eliciting a response from the computer with that address, the scanning will cause the computer to function. The trespass analogy makes more sense in a 1986-world than in a 2015-world. However, the trespass analogy, arguably, is arguably equally consistently referenced throughout the committee reports as are concepts of privacy, confidentiality, integrity and availability that support a narrower approach.

---

[758] S. Rep. 99-432 at **2484

[759] S. Rep. 99-432 at **2484

[760] This could be because there are people researching internet topology, malicious hackers looking for webservers running vulnerable software, etc. See e.g. the Ars Technica article by Dan Goodin: "Guerilla researcher created epic botnet to scan billions of IP addresses (20 March 2013), at http://arstechnica.com/security/2013/03/guerilla-researcher-created-epic-botnet-to-scan-billions-of-ip-addresses/. Last visited 18 June 2015. The article does discuss illegal research, but that particular researcher is certainly not the only one scanning IP-address for legal or illegal reasons. The following is a link to a website that enables those interested to download a program that can perform a scan of the entire IPv4 address space within a span of five minutes. https://zmap.io/. Last visited on 18 June 2015.

Construing "access" has typically not been the pivotal issue, and mostly not an issue at all, of the courts' inquiry into the CFAA. The cases typically involve confusion as to the meaning of "authorization" rather than the meaning of "access". The cases that Kerr[761] and Clough[762] use to contrast different readings of the term "access" involve two federal cases and a single state case. The narrower reading of "access" persuaded the court in *State v. Allen*[763]. In *Allen*, the defendant had repeatedly dialed up a computer belonging to Southwestern Bell Telephone that controlled long-distance telephone switches. Each time the defendant was confronted with a password prompt. For that conduct, the defendant was charged with unauthorized access in violation of the Kansas state computer crime statute. The state computer crime statute defined access in a broad manner that included even "approaching" a computer. The court refused to rely on the statute definition due to vagueness issues, and reasoned that the ordinary meaning of access was preferable. Under the ordinary meaning of access, the court held that Allen had not "accessed" the computer unless he managed to get past the password prompt. Just viewing the password prompt did not allow Allen to actually use or obtain anything from the computer.[764] Similarly, a federal district court in *Moulton v. VC3*[765] concluded that a portscan carried out against a company's computers did not constitute "access".[766]

A broader approach was adopted by the district court in *AOL v. NHCD*[767]. The case involved spammers who had harvested AOL email addresses and proceeded to send spam email to AOL email addresses in violation of AOL's terms of service. The court held that NHCD had accessed AOL's computers by sending emails that would be transmitted through AOL's computers. That is, the court argued that sending an email constituted access.[768]

---

[761] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p

[762] Jonathan Clough: Principles of Cybercrime (2010), pp. 65 et seq.

[763] *State v. Allen*, 917 P.2d 848 (Kan. 1996)

[764] See also summary of case in Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, pp. 1624-1626, and summary in Jonathan Clough: Principles of Cybercrime (2010), p. 65

[765] *Moulton v. VC3*, 2000 WL 33310901 (N.D. Ga. 2000)

[766] See summary of case in Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1626, and summary in Jonathan Clough: Principles of Cybercrime (2010), p. 68

[767] *America Online v. National Health Care Discount, Inc.*, 121 F.Supp.2d 1255 (N.D. Iowa 2002)

[768] See also summary of case in Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, pp. 1627-1628, and summary in Jonathan Clough: Principles of Cybercrime (2010), p. 67

Generally, however, very few cases involve a dispute over the meaning of access. Most CFAA cases revolve around how to construe the term "authorization". Reading access narrowly makes it possible for judges to reach a desired result, e.g. in cases where a computer is publicly accessible and the defendant has not actually had any way of using the computer in a meaningful sense because the defendant has only been able to view a password prompt. Excluding such acts from unauthorized access statutes by relying on "authorization" triggers the more difficult, and arguably more contentious, inquiry into what the owner did or did not authorize or consent to; rather than the simpler approach of excluding the act from scope, because the act did not constitute "access". However, the easier solution comes at the cost of the arbitrariness connected with determining what interaction with a computer constitutes access and what does not (as pointed out by Kerr and Clough), since all interaction is access in the technical sense. The question is whether every technical access corresponds with the concept of access in legislation, and the answer is that it depends on what perspective the court opts for in any given case.

10.6 The difference between "access" and "use"

As noted above, "access" seen from the external perspective is largely synonymous with "use", however, that is in the context of access to a computer; not access to information, since access to information does not imply use of information, whereas accessing a computer necessarily means using the computer. However, unwanted use of information obtained from a computer to which access is authorized has resulted in policies and terms that state for which "purpose" one may "access" a computer or information in order to try to craft an unauthorized access claim where the person was otherwise authorized to access the information, but did so for purposes incompatible with the interests of the owner.[769] For example, as will be discussed further in the chapter on the scope of the authorization with respect to so-called insiders, the access can be made contingent on that the access is for a specific purpose and no other, thereby obfuscating that the person in fact was authorized, but the information was used for unwanted purposes.

[769] See e.g. *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F.Supp.2d 479, 499 (D. Md. 2005) ("Although Plaintiff may characterize it as so, the gravamen of its complaint is not so much that Werner-Masuda improperly accessed the information contained in [the database], but rather what she did with the information once she obtained it. The SECA and the CFAA, however, do not prohibit the unauthorized disclosure or use of information, but rather unauthorized access.")

For example, where employers forbid employees to access a computer for non-business reasons, means that the employer is really not interested in limiting the employee's access to the computer as such, but wants to control how the employee uses the computer and information once it has been accessed. Similarly, websites' Terms of Use (ToU) or Terms of Service (ToS) could be read to do the same. That is, employers and other computer owners try to make access contingent on the person's future adherence to a set of rules that do not regulate the access as such. Access has already been granted.

Although an inquiry into "purpose for access" or "use" of a computer may seem appropriate given that our minds tend to go to the more nefarious reasons for accessing a computer one generally has authorization to access, the Ninth Circuit in *US v. Nosal*[770] (concerning theft of trade secrets) did a very good job explaining why conditions for access, or purpose of access, which typically relate to later undesirable *use of information* obtained or use of a service for reprehensible *purposes*, should not trigger the application of hacking statutes.

Nosal had encouraged former colleagues to transfer confidential information to him in breach of their employer's policy, which prohibiting accessing company computers for nonbusiness reasons. The question at the center of *Nosal* was whether the defendant had violated the CFAA by aiding and abetting the employees in exceeding authorized access with intent to defraud. Simplified, it was a question of whether an employee with authorization to access a database exceeded authorization when their purpose for accessing the computer was not business-related as required by company policy. The government's theory was that "exceeds authorized access" in the CFAA should be construed so as to mean "access for an unauthorized purpose". The court disagreed, because the government's construction would make "every violation of a private computer use policy a federal crime."[771] Checking personal email, using Facebook, playing solitaire and so on, also fall under nonbusiness use of an employer's computer. As the Ninth Circuit pointed out, doing Sudoku puzzles on paper during work hours would be fine, but doing Sudoku puzzles on the computer would be a crime.[772] Furthermore, construing "exceeds authorized access" to include use policies would also mean that violations of websites' Terms of Use could trigger criminal liability. Thus, the court held that "exceeds authorized access" is limited to violating restrictions on access to

[770] *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012)
[771] *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012)
[772] *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012)

information, not use of information.[773] Consider also the case *Koch v. John Does*[774], where the plaintiff claimed that access to a public website was unauthorized because the defendants had later used information from the website in an undesirable manner. By simply asking for what the purpose of the access is, one can attempt to conflate the concept of access to and obtaining of information with the intended later use of the information. This will be discussed further in connection with authorization as well.

In the Danish context, this distinction between *access to information* and *use of information* makes sense as well. Although the Danish hacking provision, § 263(2), relies only on "without right" for both employees and outside hackers (instead of having an additional "or exceeds authorized access" to regulate insiders), the focus of § 263(2) is access to information and programs, not access to the computer as a "thing". Later use of information that was accessed with right is not covered by the language of § 263(2).[775] Another person, who did not participate in the crime nor aided or abetted the offender, but later acquires or uses information accessed in violation of § 263(2), incurs criminal liability independently under the criminal code's § 264c. Misuse or misappropriation of specific types of information may be subject to other laws, such as trade secret statutes or data protection statutes. § 263(3) enhances the penalty for unauthorized access violations if the offender has the intent to obtain trade secrets or if the conduct is organized or systematic in nature. However, such aggravating circumstances are still hinged on a lack of authorization to access the trade secrets. Insiders are also independently criminalized in the Marketing Act § 19, which criminalizes the misappropriation of trade secrets (both acquiring trade secrets in an improper manner, use and disclosing trade secrets). There is some overlap between the Marketing Act's § 19 and the criminal

---

[773] *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012)

[774] *Koch Industries v. John Does*, 2011 WL 1775765 at *8 ("[…] Defendants were given unimpeded access to the information on Koch's public website. Koch's complaint is not that Defendants obtained the information without authorization, but rather that they ultimately used the information in an unwanted manner. The CFAA addresses only the act of trespassing or breaking into a protected computer system; it does not purport to regulate the various uses to which information may be put), *LVRC Holdings v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), *Orbit One Communications v. Numerex*, 692 F.Supp.2d 373, 385 ("The CFAA expressly prohibits improper "access" of computer information. It does not prohibit misuse or misappropriation."), *Cvent v. Eventbrite*, 739 F.Supp.2d 927, *WEC v. Miller*, 687 F.3d 199, 204, *Dresser-Rand v. Jones*, 2013 WL 3810859. And the single Danish case that indicates the same line of thought as that prevailing in US federal courts, U 1996.979Ø, 980-981 (A criminal case against a bank employee who accessed information shortly prior to his resignation; access for improper purposes, i.e. printing out confidential information to which the employee had authorized access but no business-related purpose to access, was not covered by section § 263 (2) and (3) because the employee was authorized to access the information).

[775] See different assumption in Mads Bryde Andersen: Lærebog i EDB-RET (1991), p. 312. Andersen claims that unauthorized use of information can be covered either under the criminal code § 263(2) or under copyright law. The statutory language of § 263(2) does not support that assumption, nor can support be found in the legislative history or case law.

code's § 263(2) and (3), but it is only unauthorized access to the information that is covered by the latter – not the unauthorized disclosure or unauthorized use of information. There is no language in the legislative history that indicates that unwanted use of information makes the initial access to the information unauthorized. Use and disclosure fall outside the scope of the "access" language of § 263(2) as well.[776]

Unauthorized use of things, including a computer, is covered by the criminal code's § 293(1). The 1985 Committee report clearly states that "use" of information is not covered by § 293(1) – only use of things.[777] Use of a computer for private purposes, such as maintaining a membership roster on a work computer, or even programs where a program is used to process information belonging to the user for private purposes, or where a disc with a computer program is taken home to use the program for private purposes. However, the Committee was clear in stating that it was uncertain to which extent employers tolerated such private use at the time (in 1985), and that not all private use may be prohibited. However, the Committee made it very clear that later use of information is not covered by § 293(1), noting that due to the fact that § 293(1) prohibits unauthorized use of "things", it is necessary to distinguish between use of information or programs where they are an integral part of the thing, and use of information or programs viewed as conceptual ideas.[778] In other words, use of information that one has access to through one's work does not appear to be covered by § 293(1), whereas use of the hardware and software to store or process information belonging to the employee, such as storing family photos, hobby club roster, etc. may be covered – at least by 1985's standards. However, processing and storage power today would make such things trivial, and personal use is widely accepted to some limited degree. One case where there appears to have been little room for personal use and which does not relate excessive storage or processing power usage, is a case where the possession of the privately owned data was illegal. In a Danish case, *U 2003.585/1Ø*, a police employee (an assistant police prosecutor with a local police department) was convicted of possession of child pornography on home computers and of unauthorized use of a thing for having stored thousands of pornographic images, including child pornography, on police servers. Regrettably, there is no reasoning at all in the court's decision as to how the court reached that decision under § 293(1); the only "reasoning" for the conviction is a restatement of the prosecution's indictment in a single sentence. Therefore, there is not much to learn about the scope of § 293(1) from that case alone in terms of unauthorized use of computers, since the particular factual circumstances of the case are somewhat unclear. The criminal code § 293(1) and its use against the police prosecutor may serve as an "unauthorized access to computers" provision (that does not require that information was obtained), in that the difference between access and use of a computer is ostensibly non-existent, whereas there is considerable difference between access to and use of information. However, if the defendant had authorized access to use the computer, and he uses the computer contrary to policy or stores illegal material on it, should not as such result in a

[776] In an unpublished 1996 (December 19th) decision in a criminal case from the district court in Roskilde, the court (and the prosecution and defense also agreed on this issue) argued that because unauthorized access necessarily means that the subsequent use must also unauthorized, section 263 (2) absorbs the unauthorized use (section 293 (1)). This should not be understood as if unauthorized access also means unauthorized use, so that unauthorized use can *make* the access unauthorized. This is not the case.
[777] Committee Report 1985 no. 1032, 33-34
[778] Committee Report 1985 no. 1032, 33-34

revocation of authorization based on purpose of use. The illegality of the materials stored was already criminalized. Breach of internal policy – as explained in the chapter on insiders – should not automatically revoke authorization, but should rely on contract law and labor law remedies, and the criminal law with respect to the possession of the illegal content. This avoids the need to create a strategy for how to get past the fact that the person was authorized to use the computer.[779]

10.7 Summary

Although "without right" places the primary limitation on the reach of the scope of hacking statutes, how "access" is construed is not unimportant, either. Because the conduct must fit every element of the hacking statute for the conduct to trigger the statute's application, the construction of "access" to an extent controls the relevance of "without right" in certain cases. For example, if "access" is construed narrowly so as to mean that a computer must be entered, then portscanning, pinging and the likes (maybe even access to public websites) regardless of whether the act was done without the authorization of the owner, falls outside the scope of the hacking statute. How "access" is construed is thus important, because it impacts the extent of the relevance of whether an act was done with or without right.

The Convention on Cybercrime, according to the Explanatory Report, also indicates that the appropriate approach is a middle ground between Kerr's narrow and broad constructions of "access". However, as pointed out in the chapter on authorization with respect to outsiders, the Explanatory Report exempts from the scope of illegal access, the access to publicly accessible systems, e.g. webservers that allow free and open access by the public. The drafters of the Convention and the Report do not exempt such access from the scope because it does not constitute "access" (and such an approach would, like Kerr and Clough point out, be rather arbitrary), but because such access is considered to always be "with right".

---

[779] In a Swedish case from Svea Hovrätt *RH 2015:15*, the court acquitted an employee of unauthorized access. The employee had installed a program on a work computer. Installation of programs by employees was explicitly prohibited in policy. The court indicated that the use policy was irrelevant with respect to the application of the illegal access statute. Furthermore, the court interestingly cited the 2005 Council Framework Decision as an aid to interpret the Swedish illegal access statute. In another recent Swedish case *NJA 2014 s. 221 (NJA 2014:19)*, Högsta domstolen affirmed a police officer's conviction for illegal access. He had accessed the police databases to search for information on himself. The court relied on the fact that the police officer had no work-related purpose for doing so. Whether such conduct would also be a violation of the Danish hacking statute remains to be seen.

The Council's Framework Decision and the Directive do not define "access". Therefore, there is not much to say about how a court might construe illegal access under either legislative act. However, by requiring that a security measure must be infringed for the access to trigger criminal liability (as well as the access being without right), the Directive implicitly excludes access to e.g. webservers that allow free and open access by the public. This may not be true in all cases of publicly accessible webservers, since it is regrettably unclear what is considered a security measure under the Directive.[780] However, under the Framework Decision, which ostensibly only Denmark is still bound by, it is not mandatory to restrict illegal access to only cover those acts that involve infringement of security measures.

So far, the few Danish decisions that touch upon the meaning of "access" have resulted in a construction that requires more than just causing the computer to function, which is in accordance with the explanation of "access" found in the Committee Report of 1985. However, there is insufficient data to suggest that the Danish courts or Danish legislature have adopted what Orin Kerr dubs the narrow reading, because there is, so far, no case that has excluded application of the hacking provision solely on the grounds that what was "accessed" was e.g. a public website. The Danish approach appears to be a middle ground between Kerr's broad construction of access and his narrow construction of access, because the Danish courts require the computer to have been entered, or that the person causing the computer to function did so with intent to gain entry (attempt). Under that logic, computers through which an email is routed are hardly "accessed" in a way relevant to an "unauthorized access" provision, such that it would trigger criminal liability absent authorization. However, since the Danish provision prohibits unauthorized access to programs and information, the statutory language does not strictly dictate such a result, nor is there support in the language for the result. The support for the courts' construction of "access" is found in the 1985 Committee Report, which still leaves some room for discussion where a creative and aggressive prosecutor or plaintiff desires to challenge the current construction, which ostensibly rests only on two unreported district court decisions on portscanning.

Construing "access" narrowly is tempting in order to exclude conduct that does not resemble "hacking" much; especially in light of the problems presented by "without right" that indicate that

[780] See e.g. below section on the social norms approach in the chapter on without authorization with respect to outsiders. In that section there are examples that are likely not criminal conduct, but can easily be construed as such by an aggressive prosecutor or plaintiff.

"without right" / "without authorization" actually places very few limitations on the scope of hacking statutes. US courts have often implicitly accepted a broad construction of "access" whilst interpreting "without authorization" either very broadly or relatively narrowly (compared to the broader options), leading to the CFAA being applied quite differently in similar cases where the conduct differs only as to in which jurisdiction it took place. The chapter on authorization with respect to outsiders will show that there are numerous CFAA cases involving access to publicly accessible websites in addition to the case cited above involving the sending of email constituting access to the AOL servers through which the emails passed.

Finally, there is the important distinction between "access" and "use". The distinction is not important with respect to access to and use of a computer, but it is extremely important with respect to access to information. There is an obvious difference between authorized access to information and authorized use of information. Whereas *access* merely means that the information can be obtained, *use* relates to what one does with the information later on. Use of information is already regulated by several areas of law, for example, data privacy law, trade secret law, copyright law, trademark law, and so on. For example, the *Koch* case mentioned above illustrates the difference between access and use, in that the defendants' undesirable later use of information from a public website did not mean that the access to the website was unauthorized.

11 AUTHORIZATION - OUTSIDERS

Outsiders are those lacking any authorization to access the computer (US law), or information or program (Danish law). The legislative history of the CFAA and the legislative history of the Danish hacking provision both distinguish between the situations of 1) persons who have no authorization (outsiders) and 2) those that have some authorization (insiders). The distinction, which was perhaps quite useful as a legal distinction before internet access became commonplace, has become a murkier one in a networked world where everyone in the world has some authorization of sorts to access a myriad of publicly accessible systems, be it webservers, file-sharing servers, email servers and so on. This chapter deals with the concept of (lack of) authorization as it applies to "outsiders". Nevertheless, the insider-outsider distinction is still relevant in terms of IT security, despite there not being a clear consensus about how to e.g. define "insider". Thus, the core problems related to "true" insiders, such as employees, who have privileged access to systems or information not available to the public, are still relevant. But that relationship substantially differs from the relationship between a website owner and a member of the public who happens to visit the website.

In the US, the distinction between insiders and outsiders has manifested itself in the statutory text of the CFAA; "without authorization" and "exceeds authorized access". In Denmark, "without right" applies to both insiders and outsiders, i.e. both to those that have some authorization to use the computer and those that have no authorization. Additional language such as "exceeds authorization" is not needed in the Danish hacking provision, but it is pointed out in the 1985 Committee Report that employees who exceed their authorization by accessing information that lie outside the scope of authorization have accessed the information "without authorization".[781] It is important to note that the Committee stated that not all employees who exceed their authorization are necessarily subject to criminal liability; whether the employee's act falls within our outside the scope of § 263(2) ought to be decided on a case-by-case basis.[782] The question of whether acts "exceed authorization" is necessarily dependent on the definition of "authorization", which is why authorization with respect to outsiders is taken on first.

[781] See Committee report 1985 no. 1032 at 26
[782] Committee report 1985 no. 1032 at 26

11.1 Sources of "authorization"

Authorization, in its traditional legal meaning, manifests itself mainly in consent (be it implied, express, written, oral, etc.), but authorization may in some instances also follow from statutory rights and obligations[783]. It is, however, unclear to which extent consent, or the absence of consent, and the multitude of ways consent may manifest itself is intended to regulate the scopes of criminal statutes prohibiting unauthorized access to computers, and information and programs. Several problems arise if the consent paradigm is applied unchecked in a way that allows a computer, information or program owners to exercise complete and absolute control over any and all rights to interact with the computer etc., even where the computer runs servers that allow free and open access by the public to the information.

The American "without authorization" / "without right" are not defined in the CFAA, the Danish criminal code or Convention on Cybercrime. In an attempt to shed some light on the matter, I will first analyze "without right" in the context of the Convention, since both Denmark and the United States have ratified the Convention, and furthermore, because the EU cybercrime legislation is based on the Convention. Then, I will examine what "without right" means in the EU cybercrime context, since Denmark has implemented the 2005 Framework Decision on attacks against information systems, which does define "without right". The EU Directive that repealed and amended the Framework Decision for all member states except for Denmark provides, in some respects, some significant improvements to the Framework Decision, which Denmark may or may not benefit from implementing despite not being obligated to do so. Finally, I will use US courts' interpretation and construction of "authorization" in the CFAA and the factual circumstances of the CFAA cases to show the possible reach of the Danish criminal code § 263(2). There are rather few reported § 263(2) cases and thus it is interesting to explore how broad the scope could and should be pushed as Danish court start seeing more hacking cases. "Without right" is intended to be the limiting factor of a very broadly phrased provision, but as will be shown, if the scope will be limited by "without right" depends on the courts construction of language that otherwise provides rather little guidance to those enforcing such a broad statute of what is illegal and what is not; especially,

[783] These latter types of authorizations fall outside the ambit of this article. For example, in *Edge v. Professional Claims Bureau, Inc.*, 64 F.Supp.2d 115 (E.D. N.Y. 1999), a district court held that because the defendant was allowed to obtain the information under the Fair Credit Reporting Act (FCRA), obtaining the information could not be without authorization under the Computer Fraud and Abuse Act provision that specifically prohibits unauthorized access to consumer information contained in a file of a consumer reporting agency. See *Edge* at *119.

as the scope continues to expand into new contexts in tandem with information systems being integrated in every aspect of our lives.

The subject of the following sections is therefore the source and extent of authorization based on legislative history, statutory language and case law. It will be shown that the Convention's and EU law's aspirations of harmonization of domestic substantive criminal law arguably fails to be meaningful, because the meaning of the broad key elements of the crimes have been left to the domestic legal system (in addition to the lack of harmonization of general principles of criminal law, such as mens rea, which also affects the extent of the criminalization). Leaving these core concepts to be construed differently by each signatory leads to numerous different applications of hacking statutes, even though the statutes are implementing the same Convention.

11.2 "Without right" in the Convention on Cybercrime

The 2001 Convention was created and signed after the invention of the Web and commercialization of the internet; unlike the American CFAA and the Danish provisions on computer crime[784]. The drafters of the Convention, thus, had ample opportunity to consider the implications of applying traditional trespass inspired computer crime law to a networked world where shared computers are a norm and not an exception as was the case in the 1980s. As stated before, the US had vast influence on the drafting of the Convention and the Explanatory Report due to its experience with computer crime, and according to the Department of Justice, succeeded in drafting a Convention that essentially mirrored existing US law. Denmark, like the US, has also ratified the Convention[785], and the Danish government made numerous references[786] to the text of the Convention and the Explanatory Report when commenting on the amendments to the Criminal Code and the Administration of Justice Act[787] in preparation for the ratification of the Convention, creating at least a tentative presumption that the Danish government and the legislature had some regard for the Explanatory Report as an interpretational aid. It is prudent to look at how the Explanatory report

[784] Apart from several subsequent amendments that did not particularly address the impact of the popularization of the Internet, especially in the aftermath of the invention of the Web.
[785] The US is also a signatory to the convention and has ratified it.
[786] Mostly in the context of the Convention's articles 16 and 17 regarding expedited preservation. The Explanatory Report is not binding, but the Ministry of Justice did, by relying on it for the implementation of the Convention, give it some added value, although it is still only persuasive authority at best.
[787] In Danish *Retsplejeloven*. It contains procedural rules, both civil and criminal.

defines *without right*[788], because the Convention does not itself provide such a definition. The Explanatory Report paragraph 38, states the following about "without right":

"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law."

This excerpt from the Explanatory Report explains exceptionally little. Consent, self-defense, necessity, other principles or interests, contract, and so on. Complete deference to domestic law with respect to defining the meaning of the concept that places the primary "limitation" on the scope. Nothing is excluded; everything is made possible. How differently "authorization" or "right" can be construed, is evident in CFAA cases in US law.

However, the drafters seemingly agreed, in the Explanatory Report, that not everything falls within the scope of article 2. They specifically exempted publicly accessible systems:

"The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). **Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right"**."[789]

The language of the last sentence references not what the owner allows, but what the system allows. Arguably, here it is the system that acts as a kind of proxy for the owner. If the system grants access, the access is authorized; however, whether what the system technically allows is controlling in cases where the owner has forbidden a particular user to access his publicly accessible system is unclear.

This question of man versus machine in terms of whose authorization counts is complicated by the next paragraph of the Explanatory Report. The Explanatory Report paragraph 48 addresses issues of consent with respect to one type of publicly accessible system, a webserver:

---

[788] The Convention uses the term 'without right' instead of 'unauthorized'.
[789] Explanatory Report para. 47. Emphasis added.

"**The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user.** The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the right holder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it."[790] [791]

The basis for authorization to access publicly accessible webservers is thus implied consent.[792] The text furthermore impliedly excludes hypothetical consent, which is generally, at least in Danish law, considered to have no exculpatory effect anyway. This follows from the part of the text that ostensibly requires an owner to have considered the possibility of a tool's application and arguably at least implicitly accepted the possibility of the tool's application. Nevertheless, does that necessarily mean that unexpected access to a website, or any other publicly accessible resource, is criminal just because consent cannot cover, with exculpatory effect, that which the owner has not considered and accepted as a possibility before the fact?

It is the implied authorization (consent) to access mentioned in the Explanatory Report's paragraph 48, although almost never articulated in legislation or by courts, that is taken for granted by most, and unless met with access restrictions, few people, if any at all, would think of contacting a website owner in order to acquire explicit authorization to access prior to any visit to the website.[793] However, that is not to say that consent necessarily is the appropriate basis for authorization to access public websites. The Explanatory Report's paragraph 43 lays the groundwork for the Report's subsequent discussions of the Convention's article 2 to 6, by stating the following:

"The criminal offences defined under (Articles 2-6) are intended to protect the confidentiality, integrity and availability of computer systems or data and not to criminalise legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices."

---

[790] As the Explanatory Report accounts for in the following paragraph, such a broad scope of criminalization is not undisputed. "Opposition stems from situations where no dangers were created by the mere intrusion or where even acts of hacking have led to the detection of loopholes and weaknesses of the security of systems." See the Explanatory Report, para. 49.
[791] Emphasis added
[792] Whether that was intended to be generalized to apply to all types of publicly accessible systems is not entirely clear.
[793] This interpretation was rejected by the court in *Craigslist v 3Taps (2013)* where the court rejected 3Taps argument for an 'open internet' (the court decided that was a matter for Congress to decide, *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D.Cal.), at *8) and accepts Craigslist's argument that it can revoke authorization to access to a public website on a case-by-case basis even though the website allows open access by the public in general. That is, the court condoned selective 'banning' of visitors deemed unwanted by the website proprietor.

The Explanatory Report paragraphs cited above expressly state that publicly accessible systems and resources are not protected by article 2 of the Budapest Convention, because, as paragraph 47 clearly asserts, there is no criminal act if the computer system allows free and open access by the public. Furthermore, paragraphs 44 and 48 strongly indicate that any interests beyond confidentiality, integrity and availability of computer systems or data, fall outside the intended scope of article 2. That which is publicly accessible is inherently not confidential. Thus, the computer system's access controls, as opposed to the website owner's subjective wishes or hopes, appear to be the deciding factor with respect to publicly accessible systems. Under the Convention, as interpreted in light of the Explanatory Report, contractual agreements are, arguably, relegated to governing access authorization that requires prior negotiation for authorization; that is, for access to a non-public website or other service that does not allow free and open access by the public in the sense that accessing the website grants access to *something more* than that which is accessible by the public. This is a reasonable result, because where the owner places his information out in public, the access by the public carries with it no implications for any of the protected interests at the heart of hacking provisions, namely confidentiality, integrity and availability.

11.3 "Without right" in the EU Framework Decision and the EU Directive

The 2005 Framework Decision defines "without right" in article 1(d):

"'[W]ithout right' means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the national legislation."

The 2002 proposal for the Framework Decision emphasized that it was important that certain activities, such as ordinary actions of users and legitimate scientific research, would not be criminalized when the Framework Decision is transposed into national law.[794] None of those exceptions from the scope made it into the 2005 Framework Decision.[795] Similarly, in the same proposal, the Commission concedes that "without right" is a broad notion, and it recognizes that it leaves flexibility to the member states. However, the Commission also noted that that flexibility

[794] COM(2002) 173, p. 11 (regarding the definition of an authorized person)
[795] As mentioned above in the discussion of the scope of "access", other language that narrowed the scope of the article prohibiting illegal access were also absent in the final version of the Framework Decision.

should be tempered by exemption of certain activities from the scope; namely, those activities and persons defined as "autorised person", a definition which did not make it into the final version of the Framework Decision, and thus, nor did the exceptions from criminalization contained in it that were supposed to temper the flexibility given to member states to define the scope of the offenses. In other words, the meaning of "without right" in the context of the Framework Decision is broader than that of the Convention's as interpreted in light of the Explanatory Report. This is because, as opposed to the Explanatory Report, which was adopted alongside the Convention (although it is not binding), the 2002 proposal is just a proposal, many parts of which were not adopted and its value as an interpretative aid is questionable at best. "Without right" is essentially, again, just a reference back to national law.

Article 2(d) of the Directive defines "without right" in the following way:

"'[W]ithout right' means conduct referred to in this Directive, including access, interference, or interception, which is not authorised by the owner or by another right holder of the system or of part of it, or not permitted under national law."

The language is slightly odd, again, because it equates "without right" also with the *conduct* that is not permitted, rather than just equating "without right" with lack of permission (be it the owner's or permission derived from law). The proposal for the Directive does not differ significantly from the language in the final Directive. Although the language is peculiar, in that it could be read as making "without right" redundant in an article prohibiting "access without right" because, as the definition alludes to: without right = unauthorized conduct. That reading makes little sense, and there is no reason given in the proposal for the Directive as to why the definition is phrased in such an odd manner. Reading the definition of "without right" in a way that makes redundant the usage of "without right" in the remainder of the Directive is nonsensical. Thus, for the purposes of this dissertation – and because it is arguably the way it is supposed to be understood – "without right" is read as "lack of permission under national law, or lack of authorization from the owner or other right holder" rather than being read as meaning "conduct that is unauthorized".

However, the definitions of "without right" in both the Framework Decision and Directive simply do what the Convention did (minus an explanatory report to clear things up); "without right" refers back to the national law for possible source of permission, and also so with respect to consent/permission of the owner, since what qualifies as exculpatory consent in criminal law or permission under other laws, is a question of national law, not EU law.

As discussed in the chapter on "access" in terms of the Directive, the additional requirement that a security measure must have been circumvented for the unauthorized access to fall within the scope of the Directive's unauthorized access prohibition, limits which accesses to information systems are capable of triggering the domestic implementation of the Directive's article 3 (Framework Decision's article 2). The Directive should invariably be interpreted in light of the preamble. The preamble of the Directive states the purpose of this particular legislative act. Thus, when the Directive's preamble recital 17 further excludes a variety of factual constellations, for example, if the lack of authorization is derived solely from a contractual violation (e.g. violation of terms of service, use policies, including use of an employer's computers for private purposes) [796] this places some limits on how national courts can construe the implementing provision as they are obligated by the principle of consistent interpretation to construe the implementing provision in light of the Directive's preamble as far as possible under national law (interpreting the implementing provision in light of the Directive's object and purpose as derived from i.e. the preamble). However, as noted before, Denmark is not bound by the Directive and Danish courts are not obligated to construe any provisions in light of the Directive's preamble or the Directive itself. Even so, in light of the problematic constructions of the CFAA in absence of boundaries such as those placed by the Directive's preamble, Danish courts could get ample insight into the consequences of not placing such boundaries on the scope of § 263(2), which is in some ways even broader than the broadest, often criticized unauthorized access provision in the CFAA, 18 § 1030(a)(2)(C).

11.4 "Without right" in the Danish Criminal Code § 263(2)

"Without right" in the context of the Danish criminal code § 263(2) appears to be three-faceted. First, it is a reference to an important principle of statutory construction. Second, where the owner or other right holder has consented to the access there is no crime. Finally, the Committee report alludes to a possible third facet, a reasonable expectations test to determine whether access was or was not with right. Additionally, due to the placement of § 263(2) in the chapter on privacy violations, not all information or programs are necessary protected if they are not kept private.

[796] Directive 2013/40/EU on attacks against information systems, preamble recital 17

11.4.1 "Without right" as a reference to a principle of statutory construction

As with the concept of "access", there is no definition of "without right" in the Danish criminal code section 263(2) or anywhere else in the criminal code for that matter. Yet, this is not the only provision in the Danish criminal code where the words "without right", or similar variants, appear.[797] Trine Baumbach determined in her dissertation "Det strafferetlige legalitetsprincip" (translated: "The principle of legality in criminal law") that "unauthorized", "unlawfully", "without right" and the likes, can differ in their legal substance. For example, sometimes these terms are a reference to a legal standard in another statute or doctrine[798], and, sometimes, they are a reference to the principle of statutory construction called *material atypicality*.[799] There is no doubt whatsoever, in the case of § 263(2), that "without right" is a specific reference to the aforementioned principle of statutory construction, because the Committee that drafted subsection (2) stated so explicitly in its report[800]. It should be noted though that this principle of statutory construction applies to all substantive criminal law provisions, regardless of whether a Committee or the legislature states so explicitly or not.

The Committee added in relation to the above quote from the 1985 report regarding reasonable expectations, that the provision, meaning also the term "without right", both covers situations where the person in question has *no authorization* and where the person has *some authorization* but exceeds his authorization. In a somewhat more concrete manner, the Committee explains the interpretation of "without right". The Committee explains the first facet of the use of the term "without right" in § 263(2):

"As with the other privacy violations it is deemed necessary to add the word[s] "without right" as a part of the criminal elements. Thereby it is indicated that situations may arise where one only on a case-by-case basis can determine

---

[797] E.g. the term *unauthorized/without right* also appears in the trespass provision in the Danish criminal code § 264.

[798] In Denmark the legislative history does not support interpreting "without right" in light of another legal standard or doctrine because first of all, any clear reference to another standard is absent, and secondly, the legislator has clearly stated in legislative history that "without right" is a reference to a principle of statutory construction. The US legislator was not as clear as to how the courts ought to interpret "without authorization" nor did it specifically point to any specific standard or doctrine, but a couple of Circuits have relied on the Restatement (Second) of Agency § 112 in their interpretation of "authorization" ("Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principle."). *See Shurgard v. Safeguard*, 119 F.Supp.2d 1121, 1125 (W.D.Wash. 2000) and *Int'l Airport Centers v. Citrin*, 440 F.3d 418, 420-421 (7th Cir. 2006)(relying on *Shurgard*). It is important to note though that this cessation-of-agency approach has been rejected by most circuits, but to name a few specific cases for further reading, *see* for instance discussion in *Dresser-Rand v. Jones*, 2013 WL 3810859 (E.D.Pa.) and the 9th Circuit's explicit rejection of the approach in *US v. Nosal*, 676 F.3d 854, 862-863 (9th Cir. 2012)(en banc).

[799] Trine Baumbach, *Det strafferetlige legalitetsprincip*, 466 et seq.

[800] Committee Report 1985 no. 1032 at 26

whether an act, which technically falls within the scope of the provision's language, is punishable. The aforementioned reservation will not have any practical relevance when the acts are committed by persons lacking any authorization to access the system. As far as employees are concerned the result will be the same where the employee in question has used a personal access code, which does not belong to him, and done so to gain access to information that falls outside his authorization. But there may be borderline cases where the employee has acted outside his job description, but not in such manner that he must be penalized. In such situations the word[s] "without right" indicate[] that a concrete evaluation of the situation is appropriate."[801]

When the Committee writes that it is necessary to add the term "without right" as an element of the crime, it is referring to a principle of statutory construction in Danish law called "the principle of material atypicality"[802]. The principle plays an important role in Danish criminal law. Material atypicality refers to conduct that is atypical in terms of the type of conduct the legislature intended to criminalize through a particular provision.[803] A popular example is that related to surgeons. Under Danish law, a person cannot legally consent to infliction of serious bodily harm and so even if a person has consented to such harm, the person inflicting the harm would still face criminal liability regardless of the consent. In those situations, a surgeon carrying out an invasive procedure would not and could not be exempted from criminal liability under the aggravated assault statute due to the patient's consent. Even though the surgeon's conduct constitutes infliction of serious bodily harm, his conduct is very different from that of the typical concept of aggravated assault. Because the surgeon's conduct is *atypical* with respect to the conduct intended to be criminalized, material atypicality removes the surgeon's conduct from the scope of the aggravated assault provision (assuming of course the operation served a legitimate purpose, the patient did consent if capable of doing so, and thus, is not actually an assault).[804] Like consent is a manifestation of the victim's will that can in some instances absolve the perpetrator from criminal liability, material atypicality can be thought of as a manifestation of the legislature's will to exempt the act from the material scope of a provision.[805] [806]

---

[801] Committee Report 1985 no. 1032 at 26

[802] The principle has evolved in Scandinavian criminal law over many decades. Its history will not be the subject of this article. *See more* Trine Baumbach, *Det strafferetlige legalitetsprincip*.

[803] The act does not have to be explicitly exempted from criminal liability in the preparatory works. *See* U 1970.680/1V where the stepson was acquitted of the charge of 'unauthorised use' of a vehicle belonging to his stepfather, even though the act clearly fell within the scope of the Danish criminal code section 293.

[804] See more detailed discussion in Malene Bechmann Christensen: Det strafferetlige samtykke (2008), pp. 56 et seq. There is not complete agreement among academics whether it is consent or material atypicality that results in the surgeon's conduct not being criminal.

[805] The principle can be seen as a "not a crime because of the will of the legislator" whereas consent can be seen as "not a crime because of the will of the victim". Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 535, note 210

Vague and broad criminal provisions, although never preferable, especially in terms of reasonable foreseeability, are sometimes necessary to criminalize acts, which are not easily defined using precise terminology. The Danish hacking provision, just like its Convention and US counterparts, is a prime example of such a broad and unclear provision, characterized by its ability to catch all sorts of acts, many of which the legislature, in 1985, could not have predicted and may not necessarily have intended to criminalize. The Danish Committee's choice to include the words "without right" in section 263 (2) signals both the acknowledgment of the lack of clarity of the provision and serves as a special notice to the judiciary that whether conduct is "without right" should be determined on a case-by-case basis, because acts that are covered by the statutory language may sometimes lack the characteristics of the type of crime intended to be criminalized[807].[808]

11.4.2 "Without right" as a reference to lack of consent

There is little mention in the Committee report of consent as a source of "right". However, that is not required as such because the words "without right" in the context of section 263(2) (and similarly in the trespass provision in § 264) imply that the owner can authorize others to access her information and/or programs – making their access authorized. Generally, consent is a defense to many privacy violations. Therefore, both consent and material atypicality act as limitations to the broad scope of the Danish hacking provision; one representing the victim's will and the other the will of the legislature.

---

[806] Sometimes the Ministry proposing the bill gives examples of such situations in the bill or a Committee does so in its reports.

[807] Trine Baumbach: Det strafferetlige legalitetsprincip (2008), p. 468

[808] Generally speaking, for an act to incur criminal liability under any given criminal provision the act must fall within the scope of the description of the actus reus, mens rea and additionally the act must be unlawful (absence of any defence, excuse or justification that alleviates criminal liability for an otherwise criminal act). In Danish law it has both been argued that, systematically, the material atypicality principle is associated with the actus reus requirement and also that it is associated with the 'unlawful' requirement. Baumbach argues in her dissertation "The principle of legality in criminal law", and I agree, that it is not immaterial whether the principle concerns the former or the latter. On the one hand, if the principle came into play as part of the "unlawful" analysis, it has already been legally concluded that the defendant committed a crime, and the "unlawful" analysis serves only to determine whether the defendant had a legally relevant excuse for committing the act that may exempt her from penalty. On the other hand, if the principle is associated with the actus reus analysis, "material atypicality" is not treated as a legal excuse for committing a crime, but as a reason for the absence of actus reus – meaning there was no criminal act.

11.4.3 A "reasonable expectations test" as a construction of "without right"

As mentioned, § 263(2) is placed in the Danish criminal code's chapter on privacy violations. The chapter consists of rules addressing prohibited acts such as criminal trespass (§ 264), defamation (§ 268), and the unauthorized photographing of persons on non-public property (§ 264a). In the Committee's 1985 report, the Committee states the following in relation to § 263(2) and its placement in the chapter on privacy violations:

"As with the other privacy violations, violations of the suggested provision will comprise a person gaining access to something, which with respect to them can **reasonably be expected** to be a restricted area, that is, inaccessible."[809]

The concept of reasonable expectations, although in many ways appropriate as a test in privacy contexts in the physical world where we have had hundreds of years to figure out the line between the acceptable and unacceptable with regards to trespass, is problematic in a highly interconnected world where sharing computers is the norm and information is often made publicly accessible, e.g. on the web. Conceptually, the reasonable expectations test is a question of social norms and the ability and possibility of observing and deducing limitations on conduct in a given context. Those norms have not been created or discovered yet with respect to the law in a computer context. There is no Danish case law that could clarify how such a reasonable expectations test would work in practice in a computer context or in the broader internet context. An American federal appellate court, however, has addressed a question of viability of a reasonable expectations test in a computer and internet context, and the case shows that reasonable expectations in a computer context, especially an Internet context, is far from being a settled matter, or even an easy matter to resolve.

In *EF Cultural Travel v. Zefer*[810], the First Circuit rejected a "reasonable expectations" test that had been applied by the district court stating amongst other things that such a test would be a "highly imprecise, litigation-spawning standard"[811]. The district court's test of "reasonable expectations" entailed, essentially, that the lack of authorization to access could be inferred from the

[809] Committee report 1985 no. 1032, p. 25. Emphasis added.
[810] EF Cultural Travel v. Zefer Corp., 318 F.3d 58 (1st Cir 2003). The test which was proposed by the district court was based on the following factors that the district court found to be circumstances from which "lack of authorization could be inferred": "the copyright notice on EF's homepage with a link directing users to contact the company with questions; EF's provision to Zefer of confidential information obtained in breach of the employee confidentiality agreements; and the fact that the website was configured to allow ordinary visitors to the site to view only one page at a time."
[811] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003)

circumstances.[812] This may be true in certain situations as will become apparent in the section on "without authorization" in US law. Social norms do affect the analysis of authorization, but the analysis of the connected cases *Zefer* and *Explorica* shows that a reasonable expectations test is far from appropriate where there is no norm to tie into the reasonable expectation. The *EF v. Zefer* case concerned the scope of an injunction against EF's competitor Explorica regarding Explorica's use of EF's public website to obtain price information. Zefer had designed a "scraper" (or "bot") for Explorica, the purpose of which was to scrape[813] price information from EF's website so Explorica could compete more efficiently with EF's student tour prices. Zefer had used "codes" for destinations and departure locations, which were an element of the URL, to accumulate the price information automatically and more quickly than if done by manual browsing of the website. EF contended that these "codes" were proprietary confidential information obtained by Explorica from a person bound by a confidentiality agreement with EF. The "codes", however, were easily visible to anyone paying attention to the URL (for example, "BOS" for Boston as the city of departure or destination). Thus, some manual browsing whilst observing the URL could easily have enabled a person, given they had the sufficient interest in doing so, to decipher and generate a list of those "codes", because the "codes" were visible to anyone, and then interpret their meaning based on the surrounding information. When finding in favor of EF and granting the injunction against Explorica, the district court (whose decision was being appealed) argued that lack of authorization could have been deduced from the three circumstances in the case. First, the copyright notice on EF's website that referred users to contact EF with questions. Second, Zefer, who made the scraper, had constructed the scraper with the help of supposedly confidential "codes". Third, that ordinary users of the website would have to click through it one page at a time.[814] From those circumstances Explorica and Zefer should have deduced that their *manner* of access was unauthorized and their subsequent *use* of the information was unauthorized. The court never really asked whether the defendants were authorized to access the public website, but just considered *how* and *why* they

[812] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003). E.g. that because dropdown menus were present on the website, changing the URL to navigate would be unauthorized access because the user should expect to be bound to use hyperlinks and dropdown menus when provided and thus not use any other method of browsing the website.

[813] In order to understand what the act of scraping price information entails in this case, imagine, for the sake of convenience, the more relatable action of copying prices from a publicly accessible website and pasting them into a file on your local machine. The scraping in the EF cases was simply automated. Automation of redundant tasks does not indicate "malice" or something of the sort; an integral part of the purpose and art of programming is to avoid the redundancy of manual operations.

[814] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003)

accessed the public website, regardless of the fact that anyone in the world could access the price information Explorica and Zefer obtained from the website.

The First Circuit upheld the injunction on the grounds that Explorica had misused the supposed confidential "codes" and, thus, Zefer was prohibited from assisting Explorica in violating the injunction. But the First Circuit very explicitly rejected the reasonable expectation test applied by the trial court because the test had no support in the legislative history and, furthermore, that such a test would not be "prudentially sound".[815] First, the copyright symbol did not protect the information in question, and thus, had not, like the district court argued, dispelled any notion of presumption of open access to the website and the information. Second, the presence of hyperlinks and dropdown menus, which of course the scraper did not use since it accessed the website by supplying URLs, were not technical restraints that suggested that a website could not be accessed at higher speed by not using hyperlinks and dropdown menus provided by the website owner.[816]

Incorporating such a reasonable expectation test, at least in the form proposed by the district court in *Explorica*, in a context where a norm is non-existent, would truly make anyone criminally liable, because any plaintiff, or the prosecution for that matter, can argue that hyperlinks ought to have been used, or that a defendant was obligated to ask permission regarding subsequent use of information because of the presence of a copyright symbol, even where the information that the defendant used was not protected by copyright law. Combined with the website owner's objection to the manner of access and the purpose of the access, there would be no way for anyone to avoid incurring criminal liability, even where the open web creates a strong presumption for authorization to access information on public website. The court, however, explicitly stated that its opinion was not based on a "presumption of open access to Internet information"[817], but merely on the fact that EF could have banned scrapers in its terms, but did not.[818] That is, the First Circuit, in dicta,

---

[815] *EF Cultural Travel v. Zefer Corp.* at 63 ('We agree with the district court that lack of authorization may be implicit, rather than explicit. After all, password protection itself normally limits authorization by implication (and technology), even without express terms. But we think that in general a reasonable expectations test is not the proper gloss on subsection (a)(4) and we reject it. However useful a reasonable expectations test might be in other contexts where there may be a common understanding underpinning the notion, cf Terry v. Ohio, 392 U.S. 1, 9, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968) (Fourth Amendment), its use in this context is neither prescribed by the statute nor prudentially sound.')

[816] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) and *EF Cultural Travel v. Explorica*, 274 F.3d 577, 580-581 (1st Cir. 2001)

[817] *EF Cultural Travel v. Explorica*, 274 F.3d 577, 580 (1st Cir. 2001)

[818] *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003) ("Instead, we think that the public website provider can easily spell out explicitly what is forbidden and, consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like "reasonable expectations." If EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions."). But see also *US v. Drew*, 259 F.R.D.

indicated that EF could have restricted authorization to access the website by automatic means, by writing in its terms that it banned the use of scrapers (a *manner* of accessing otherwise publicly accessible information). Were the reasonable expectation test applicable to Explorica, Explorica would be liable under the CFAA regardless of their use of a scraper; EF would have resented the *purpose* of Explorica's visits to the website, regardless of *how* the information was accessed.[819] Ultimately, the injunction stood only because the codes were obtained from a person, seemingly, in violation of their confidentiality agreement with EF.

The First Circuit's rationale behind the decision to reject a reasonable expectation test, at least in that context, is valuable also in the Danish legal context, because it exposes the problems that such a test would pose in the context of public websites where the information is freely accessible to anyone. However, the district court applied their reasonable expectations test in a way that was not reasonably foreseeable at all given the context, because there was, as the First Circuit noted in *Zefer*, no common understanding underpinning the notion; that is, there was, and still is, no social norm that morally obligates anyone to ask for permission to use information that is publicly accessible and not protected by e.g. copyright law. Similarly there is still no social norm to the effect that a person is obligated to use dropdown menus and hyperlinks unless specifically authorized to navigate differently. If a person is obligated to adhere to social norms under the threat of criminal law, then those norms must actually exist and not be tortuously created on a case-by-case basis to extend criminal law coverage to any and all conduct that is subjectively undesirable, annoying or inconvenient, to the website owner. There is no reason to assume that such a reasonable expectations test will fare any better or would prove any more applicable, appropriate or prudentially sound in the same context in Danish criminal law than in US law. There still would be "no common understanding underpinning the notion"[820].[821] The key to a reasonable expectations

---

449 (C.D. Cali. 2009) declining to impose criminal liability for intentional breach of terms of service of a website under 18 USC § 1030 (a)(2)(C), e.g. at 467 ("if any conscious breach of a website's terms of service is held to be sufficient by itself to constitute intentionally accessing a computer without authorization or in excess of authorization, the result will be that section 1030(a)(2)(C) becomes a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet*]." City of Chicago*, 527 U.S. at 64, 119 S.Ct. 1849.")

[819] At 63 ("Needless to say, Zefer can have been in no doubt that EF would dislike the use of the scraper to construct a database for Explorica to undercut EF's prices; but EF would equally have disliked the compilation of such a database manually without the use of a scraper tool. EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns.")

[820] *EF Cultural Travel v. Zefer Corp.* at 63

[821] Arguably, a reasonable expectation test has already been rejected by Danish courts in a context closely resembling the American cessation-of-agency cases, namely the case *U 1996.979Ø* (see note 24 above) from which it could tentatively be inferred that because the court held that the employee was authorized to access, and that the court did not

test is the existence of social norms. Absent social norms (that is, absent a common understanding amongst those regulated by a law criminalizing violation of some social norms), a conviction based on a "reasonable expectations" test is necessarily based only on arbitrary criteria that would offend a principle of foreseeability of application of criminal law. If the social norms do not exist, then the criteria for conviction do not, either, and thus, any criteria the court comes up with, and labels as "reasonable expectations" without those expectations being recognized by society, is arbitrary.

Furthermore, especially involving publicly accessible internet resources, and also in other contexts where access is not restricted in a meaningful way, the reasonable expectations test would not really promote the general purpose of the statute; protecting privacy and supplement the security of computers. This is because privacy and confidentiality are inherently lost when information is made publicly accessible. Under other privacy provisions in the same chapter, leaving communication, such as letters, in an area which is travelled through by other people, protection of privacy under the criminal law is lost, because this could indicate that the owner of the letter no longer cares to keep the letters to himself.[822] Thus, the protection of criminal law can be forfeited under certain circumstances where a person acts in a manner that is in contradiction to a desire to keep the information private. If the privacy protection in criminal law can be forfeited for private letters left in public where, in comparison to the Internet, a limited number of people will pass through, certainly, information made publicly accessible on the Internet equally causes a forfeiture of the privacy protection in criminal law. The presence of a copyright symbol, hyperlinks and dropdown menus cannot resurrect criminal law privacy protection against unauthorized access to the information that is publicly accessible.

It is, then, not unreasonably to consider whether lack of security perhaps influences the outcome, if the absence of security is found to indicate forfeiture of criminal law protection or that its absence leaves the material freely accessible to the public; also the absence of security may at least make for a more lenient sentence for a defendant.[823] As has been the case with every Danish committee

---

address, much less accept, the prosecution's argument that the employee probably could reasonably expect that his authority to access would be revoked immediately upon his resignation (presumably due to it being a general policy to revoke such authorization when dealing with employees with access to confidential information). The court had an open invitation to employ a kind of reasonable expectations test but it did not accept that invitation in this context – which makes it that much more unlikely that Danish courts would be tempted to introduce a reasonable expectations test in the context of publicly accessible websites where there is far less probability of consensus as to what to reasonably expect.

[822] See Committee Report on privacy 1971 no. 1601, pp. 26-27

[823] Committee Report 2002 no. 1417, pp. 25-26 (The ad hoc Committee argues that it is best if criminal law protection only plays a role where implemented security measures proved to be insufficient. At the sentencing phase, the courts

report relating to cybercrime, the Committee emphasizes in its report, 1985 no. 1032, that ensuring that effective security measures are in place undoubtedly has a far greater preventative effect than merely changing the criminal code to cover computer crimes.[824][825] These considerations imply that in the absence of security measures, the preventative effect of criminalization is little[826]; criminalization may arguably have some deterring effect[827], but it does not in any way provide or increase the actual technical security. The law is reactionary and not directly preventative in its nature compared to computer system owners' implementation of security measures. However, as is evident from the statutory language, circumvention of a security measure is not an element of the crime. But under certain circumstances, arguably, primarily where the information is publicly accessible, the owner may lose his right to protection under criminal law, because there is no longer any privacy to protect.

To summarize, very little is known about the scope of "without right" in the context of § 263(2) other than how it applies to classic instances of hacking, where an outsider, with no authorization to access the information in question, has attempted or succeeded in infringing security measures protecting information that the system does not make publicly accessible.[828] Danish hacking cases

---

then take into consideration whether there was adequate security and monitoring, or whether the lack of the same increased temptation due to lower risk of discovery, and enabled the offense to become especially serious. Of course, as noted by the Committee in the same report, organizations are not expected to be able to foresee and prevent exploitation of unknown security vulnerabilities.)

[824] Committee Report 1985 no. 1032, p. 17

[825] This is not unique to the Danish committee report, but has also been emphasized in the Explanatory Report to the Council of Europe's Convention on Cybercrime (hereafter the Explanatory Report) and, in US law in Senate Report no. 99-432 considering the amendments to the federal Computer Fraud and Abuse Act (CFAA).

[826] An almost identical statement is found in the Explanatory Report paragraph 45, which states: "The most effective means of preventing unauthorized access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorized access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above." A similar statement can also be found in Senate Report no. 99-432 at 3, which states: "It is clear that much computer crime can be prevented by those who are the potential targets of such conduct. The ABA report indicated that while the respondents to the survey overwhelmingly supported a Federal computer crime statute, they also believed that the most effective means of preventing and deterring computer crime is 'more comprehensive and effective self-protection by private business' and that the primary responsibility for controlling the incident of computer crime falls upon private industry and individual users, rather than the Federal, state or local government. The Committee strongly agrees with these views." (Citations omitted) See also the committee report 2002 nr. 1417, p. 26 et seq., which clearly states that criminal law measures, should only come into play when the victim had implemented an adequate level of security measures. That is, criminal law measures were meant to be supplementary to a responsible IT security policy and implementation of security measures.

[827] The deterring effect of criminalization is a discussion I will leave to others, as it falls outside the ambit of this article.

[828] See e.g. *U.2002.1064V* (attempted unauthorized access through use of a program called "Hack A Tack") and *TFK2015.612* (unauthorized access to computers of 47 people over a period of one year through use of a program called "Netwire")

are few, and the courts almost without exception do not give much insight into their reasoning for the particular result other than by simply restating the facts.

I will return to the subject of reasonable expectations as an approach to construe "without right" after I have used US case law to show why such an approach is preferable in comparison to several alternative approaches, all of which will be explained below in the sections on authorization with respect to insiders and outsiders.

11.5 "Without authorization" in the CFAA

Although the circuit split is most prominent with regard to when and whether misbehaving employees' conduct should trigger CFAA liability, there is not total disagreement as to how to deal with outsiders. However, that is not to say that US federal courts interpret the CFAA the same with respect to outsiders. There is no definition of authorization in the CFAA. There is only a definition of "exceeds authorized access", which inherently relies on the meaning of the concept of "authorization" in the first place.

In terms of the wide variety of situations the CFAA is applied to now, at least one commentator has suggested that the extensive application of the CFAA in civil cases may have led to a far more expansive interpretation of the provision than intended since it is primarily a criminal statute.[829] As a criminal statute, the interpretation and construction of the CFAA should have been subject to the rule of lenity even when applied in civil cases, because the construction in civil cases applies equally in criminal cases. That is, the facts that are found legally relevant to determine whether unauthorized access incurs civil liability, will also become legally relevant to determine whether access was unauthorized in criminal cases. Seeing as the fair notice requirement is stricter with respect to criminal statutes than civil statutes, this complicates the applicability of the broad constructions, such as that allowed under the contract-based approach and agency-based approach.

[829] Ian Walden, Computer Crimes and Digital Investigations (1st edn Oxford University Press 2007) 58 ("Such civil actions can greatly facilitate judicial consideration of a statute, potentially enhancing legal certainty and strengthening the deterrent impact of such legislation. Conversely, granting victims an explicit right to bring an action may result in it being used in situations not originally envisaged by legislators, thereby over-extending the reach of criminal law; as has recently been noted by a court: Because the CFAA has largely been addressed in the civil context, courts may be adopting a more expansive view of 'authorization' than they would have taken in the criminal context." Citing *Lockheed Martin v. Speed* at FN11. *See also* on a similar note Orin Kerr, Cybercrime's Scope, 1641

There are some competing approaches to construing authorization that will be analyzed in the next few sections.

11.5.1 A code-based approach

Circumvention of code restrictions, e.g. in the form of password prompts, is arguably at the core of the provision, because circumventions of password prompts are the examples that were used in legislative history. The Committee reports, relating to the CFAA, discuss employees who use the password of another to gain access to information or computers that they do not have authorization to access themselves.

Although the legislative history does not explicitly reject broader readings, as such, this section will show that a purely code-based approach, the very core of the CFAA, regardless of whether other approaches exist in the penumbra, is itself unclear and calls for arbitrary decision-making, as well as that the code-based approach does not account for convictions for accesses that society would normally view as unauthorized, but which are not prohibited through code.

Orin Kerr[830] and Patricia Bellia advocate for a code-based approach in construing authorization in the CFAA. However, even though Kerr and Bellia seem to refer to access restrictions and exploitation of vulnerabilities, many things can be viewed or construed as code restrictions and not all alleged code restrictions are remotely effective as security measures. Recall the argument of the plaintiff in *EF v. Explorica* that manipulating the URL instead of using the hyperlinks and dropdown menus was circumventing technical restrictions. However, no one would perceive hyperlinks and dropdown menus as access restrictions, because they are inherently ineffective as such and not recognized as such. Construing "code restrictions" in a broad manner, as some courts seem to have done[831], dissipates the need to inquire whether the code restrictions are really effective and meaningful as access controls. Whether Kerr means that the code-based approach for which he advocated means that code restrictions need only be more or less symbolic to resolve a notice issue, or whether the code restrictions need to constitute effective and recognized security measures is unclear. As will be shown below, relying on a broad understanding of a code-based approach for construing authorization calls for arbitrary inclusions and exclusions from the scope of unauthorized

[830] Orin Kerr has recently modified his stance in a 2015 draft paper. See the section on the social norms approach below.
[831] E.g. *Craigslist v. 3Taps*,

access statutes that do not require e.g. circumventions of effective security measures. That is, a code-based approach for construing authorization narrowly, suffers from the same arbitrariness that Kerr argues makes reading "access" narrowly unviable. Code-based approaches could in many circumstances call for reliance on a form of "social norms" that do not really exist (cf. the section above on "reasonable expectations"). Similarly, a narrower view of the code-based approach to construing authorization – i.e. requiring that the code restrictions are bona fide security measures – misses some instances of unauthorized access that are not prohibited through code, but nonetheless should still be considered unauthorized even though "code allowed the access".

11.5.1.1 Unexpected and undesired access

The beginning of what is ostensibly, but not entirely, a code-based approach appeared in 1991 in the Second Circuit with *US v. Morris*[832]. Morris had been charged with violation of § 1030(a)(5)(A) (intentionally accessing federal interest computers without authorization and damaging or preventing authorized use of information on such computers). Morris released a "worm"[833] onto the embryonic internet. The worm was coded to self-propagate and caused computers on the internet (in 1991 the internet consisted mostly of educational institution and military computers) to crash. Morris had exploited security vulnerabilities to prove that security on the internet was insufficient. The defendant knew that if multiple copies of the worm infected the same computer it would cause the computer to crash. Therefore, he had programmed the worm to determine whether the computer was already infected. In case of the worm being discovered and computers being programmed to indicate that the computer was already infected with the worm, Morris programmed the worm to infect a computer every seventh time the computer would signal that it was already infected. However, the number of times the worm would check for an existing infection greatly exceeded what Morris had expected, and computers crashed on a nation-wide scale.[834]

---

[832] *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991)

[833] Cisco's website defines "worm" as follows: "Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate. To spread, worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided." Definition available at Cisco's website at http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#5. Last visited on 30 August 2015.

[834] See summary of facts in *United States v. Morris*, 928 F.2d 504, 505-506 (2nd Cir. 1991)

Morris had exploited vulnerabilities in the early email client "SEND MAIL", in the finger daemon, and in the trusted host feature, as well as having brute-forced password restrictions (roughly describable as high-speed password guessing).

Since Morris had authorization to access and use internet-connected computers at Cornell, Harvard and Berkeley, and since he was authorized to send emails to other computers on the internet through the SEND MAIL client and inquire about other users through the finger daemon, the court asserted that it needed to determine whether dissemination of the worm was "without authorization" or in "excess of authorization". The court concluded that Morris' conduct was "without authorization", because he did not use the SEND MAIL client or the finger daemon "in any way related to their intended function". He had exploited security vulnerabilities that gave him greater privileges on other computers, some of which he had no authorization to access.[835]

As Kerr argues, the intended function test applied by the Second Circuit "appears to derive largely from a sense of social norms in the community of computer users. Under these norms, software designers design programs to perform certain tasks, and network providers enable the programs to allow users to perform those tasks."[836] Kerr furthermore notes that the test ostensibly focuses on "objective rather than subjective concerns". The intended function seems to be "what the program itself (and its supporting literature) claims that the program does."[837] However, other circuit courts have relied on, what appears to be a distorted version of the Second Circuit's objective intended function test; namely, a more subjective version of the intended function test in order to conclude that the conduct that the owner views as undesirable goes against the computers intended use, or to argue that the subjective motives of an employee when he accesses his employer's information can contravene the "intended use" of the computer (the latter being an approach discussed separately in the chapter on insiders). See more below and in the chapter on insiders.

Although the Second Circuit's use of the intended function test to include exploitation of vulnerabilities to propagate a worm, which is an objective inquiry of sorts, the "intended *function* test" is not necessarily useful or consistent if it is "misapplied" as a subjective "intended *use* test". For example, consider EF's argument in its case against Explorica that hyperlinks and drowdown

---

[835] *United States v. Morris*, 928 F.2d 504, 510 (2nd Cir. 1991)
[836] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1632
[837] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1632, note 156

menus were technical restrictions, and that using a scraper to "bypass" those restrictions contravened the intended purpose of websites, because a person could not manually click through the site with the speed of a scraper. Most commercial websites are not created for the benefit of programs accessing the website automatically, but for people using the site manually. Is scraping illegal access then because most websites are not "intended" to serve bots, but to serve humans? Technology can be used in many unexpected ways without it always being undesirable to a particular owner.

US v. Phillips, a case from the Fifth Circuit, is not really a pure code-based approach, either. Rather it seems to be a curious blend of code-based, contract-based and a social norms approach. Phillips was charged with violating §§ 1030(a)(5)(A)(ii) and (B)(i). The Court relied, it seems, on both *Morris* and *EF v. Explorica*. Phillips, a computer science student at the University of Texas at Austin (UT), had upon his admission to the university, signed an "acceptable use" computer policy, in which Phillips agreed not to conduct port scanning using his university account. He violated the computer use policy by running port scans against various computers.

The UT maintained a system called TXClass Learning Central, used by faculty and staff for enrollment related matters. Authorized users needed only enter their social security number (SSN) into a field on the login website to gain access to the site. Phillips wrote a Java program that would enter a number from a range of SSNs that is used to assign SSNs to people born in Texas (later he refined it to SSNs assigned to people born in the ten most populous counties in Texas) sequentially[838], and then retrieve the personal information associated with the SSN (if the SSN existed in the database). That way, over a period of fourteen months, Phillips obtained data related to 45,000 people.[839] Because Phillips' program queried the server rather rapidly, the UT computer system crashed several times.

Phillips argued on appeal that his access to the TXClass login page was authorized, and as a subsidiary argument that he was authorized to access TXClass' login page as an ordinary user of the

[838] The formula was publicly available according to a CNET article (7 February 2007) by Declan McCullagh at http://news.cnet.com/Police-blotter-Texas-student-guilty-in-SSN-hack/2100-1030_3-6155425.html. Last visited 20 June 2015.

[839] The summary of fact in the appellate courts decision is rather sparse. Some facts are described in more detail in a CNET article (7 February 2007) by Declan McCullagh at http://news.cnet.com/Police-blotter-Texas-student-guilty-in-SSN-hack/2100-1030_3-6155425.html. Last visited 20 June 2015.

web, and that his retrieval of information from the database was thus merely "exceeding authorized access". The court rejected both arguments.

First, the court argued that the scope of authorization to access on the basis of "the expected norms of intended use or the nature of the relationship established between the computer owner and the user".[840] The court cited *US v. Morris*, *Theofel v. Farey-Jones*[841], and *EF v. Explorica* as support. The court used *Morris* to show that exploiting vulnerabilities and password guessing was not related to the intended use "of computer systems" (the *Morris* court argued "intended *function*" in relation to Morris' exploitations of vulnerabilities in programs and protocols, not the *use* of the "computer system" as a whole, a concept much broader than "program"). Of course, only requiring a user to login with their SSN, the formula for which is publicly available, is a vulnerability – but it is not the kind of vulnerability like the security vulnerabilities exploited by Morris, because guessing a password does not contradict the intended function of a password prompt, per se. Furthermore, the Second Circuit in *Morris* did not apply the "intended function" test in the context of the brute-force attack aspect (password-guessing) built into Morris' worm; it did so with respect to the exploitation of the security vulnerabilities in SEND MAIL and the finger daemon. Entering login credentials, even if the credentials are ill-gotten, is still in line with the intended function of a login screen; namely, the entering of login credentials. Thus, the Fifth Circuit's "intended use" test is not an application of the more objective "intended function" test in *Morris*, because the Fifth Circuit focuses on subjective illegitimacy of access. The login page and protocol did exactly as they were designed to do (even if the system owner has chosen easily obtainable access credentials), regardless of whether the access credentials were legitimately obtained or not. The Fifth Circuit then used *Theofel* to argue that use of a third-party's password by an outside hacker was a type of conduct the CFAA covered; this reference makes the Fifth Circuit's misapplication of the Second Circuit's "intended function" test essentially superfluous, since it also provides support for concluding that password-guessing is in violation of the CFAA. Furthermore, the part of the Ninth Circuit's *Theofel* decision that the Fifth Circuit relies on, refers back to the Second Circuit's discussion of password-guessing in *Morris*, which is unrelated to the "intended function test". Finally, and perhaps most curiously, the court cited the First Circuit's decision in *EF v. Explorica* as support for a "reasonable expectation test", which, as may be recalled, merely provided a summary

[840] *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007)
[841] *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004)

of the district court's decision in the First Circuit *Explorica* decision; the First Circuit did not actually ever apply the test in *Explorica*. The injunction against Explorica rested on the use of supposedly "confidential codes", and the summary of the district court's test is dicta. Rather, and importantly, the First Circuit expressly rejected the district court's particular application of the test a couple of years later in *EF v. Zefer* (Zefer was the company that created the scraper for Explorica), which was decided three years before the Fifth Circuit's decision in *Phillips*. It is impossible to know whether the Fifth Circuit simply missed the *Zefer* decision. The First Circuit rejected the "reasonable expectations test" in the specific context before it, but it did not technically rule out the possibility that a reasonable expectations test could be appropriate in other contexts insofar as there is a common understanding underpinning the notion; i.e. that a social norm exists. This will be discussed in the section on social norms below.

The Fifth Circuit thus concluded that Phillip's "brute-force" Java program "was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computer data that he was not permitted to view or use."[842] The Fifth Circuit thus combines the *Morris* "intended function" test with the "reasonable expectations" test proposed by the *Explorica* district court that was expressly rejected by the First Circuit on appeal in *Zefer* in the context the district court had applied it. The first test was, arguably, misapplied and the latter test's application rejected by the circuit court in the circuit where the test was proposed by a lower court. When reading the decisions that the Fifth Circuit relied on and comparing those to the court's argument in *Phillips*, there is an unexplained and rather confusing incoherence in the court's reasoning for the outcome, although the outcome appears correct.

Regarding Phillips' subsidiary argument, the court rejected that Phillips had merely exceeded his authorized access as an ordinary internet user. The court argued that authorization typically arises out of contractual or agency relationships,[843] and since Phillips was never granted access to TXClass, but only those UT services mentioned in the use policy that he signed upon his admission to UT, then his access was unauthorized, and not in excess of authorization. In other words, even though Phillips had access to the TXClass login page like any other web user, he had never been granted authorization to access TXClass. He was an outsider, not an insider with respect to

[842] *United States v. Phillips*, 477 F.3d 215, 220 (5th Cir. 2007)
[843] *United States v. Phillips*, 477 F.3d 215, 221 (5th Cir. 2007). See more on the contract approach below, and the agency approach in the chapter on insiders.

TXClass. Recall that the First Circuit in *Explorica*, basing its decision on use of confidential information, held that it was "exceeding authorized access", not access "without authorization". However, *Explorica* involved publicly accessible information that was obtained more efficiently than users would be able to obtain manually, whilst the information obtained by Phillips were not publicly accessible on the website (*Explorica* was about undesirable efficiency of access, and in *Phillips* there was no authorization to access at all). It makes the Fifth Circuit's reliance on *Explorica* a little confusing, since the facts are easily distinguishable (and in fact very different) from the facts in *Phillips*; faster browsing than other users vs. access to information that the defendant clearly had no authorization to access.

The case illustrates fairly well the absence of a consistent method of explaining why conduct is in violation of a hacking statute. Given the facts of the case, Phillips did violate the CFAA, at least with respect to his access to TXClass, but the court's reasoning for its conclusion is not entirely sound. Rather, the Fifth Circuit's reasoning would have been vastly more persuasive, and coherent, if it had simply relied on the Second Circuit's discussion of password-guessing in *Morris* and sought additional support in the Ninth Circuit's adoption in *Theofel* of the Second Circuit's reasoning, rather than entangling itself in the use of borrowed tests that had been applied in other contexts.

The Third Circuit faced a similar, but not entirely identical, factual situation to Phillips' in *US v. Auernheimer*. The cases are not really technically distinguishable as such, but their end results differ substantially for reasons that a code-based approach cannot explain.

In 2010, AT & T was the exclusive provider of data contracts to iPads with 3G capabilities. The customers registered their accounts on AT & T's website and in the process they were assigned a user ID as well as they would choose a password, both of which the customers would need for future access to the accounts. The user ID assigned was the customer's email address. In order to make logins easier, AT & T configured their server to pre-populate (automatically fill out) the user ID field on the login page with the customer's email address. This pre-population was possible because the customer's email address was associated with the iPad's SIM-card ICC-ID[844]. The server would detect the ICC-ID, and if it belonged to a customer, it would redirect the customer

[844] "An ICC-ID is the unique nineteen- or twenty-digit number that identifies an iPad's Subscriber Identity Model, commonly known as a SIM Card. The SIM Card is the computer chip that allows iPads to connect to cellular data networks." *US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.)), at *1. Furthermore, the ICC-ID is an open standard (ISO/IEC 7812) the documentation of which is available to anyone.

away from the general login page to a specific login page, the URL of which would be "unique" in the sense that the ICC-ID would appear as an element of the URL. The email address of the customer would automatically appear in the user ID field on this specific login page.[845]

Spitler, an online acquaintance of Auernheimer, had an AT & T account but did not own an iPad (he had purchased an iPad SIM Card to try to use it on another device). In his endeavor to register the SIM Card in absence of an iPad he had researched the iPad's operating system and found the AT & T registration URL, and realized that one of the variables of the URL was the ICC-ID assigned to the iPad's SIM-card. Spitler then entered the URL into his browser, which he had configured to identify itself as an iPad using a Safari browser[846], along with his ICC-ID typed into the URL. He then noticed his email address was pre-populated in the user ID field on the login page, and he correctly deduced that the server associated his SIM-card's ICC-ID with his email address. He tested his theory a few times by manually changing the ICC-ID in the URL and found that the server pre-populated the user ID field with different email addresses.[847] Thus, the server was coded in a way that it would leak the email addresses and ICC-IDs to anyone visiting the publicly accessible website who also got the idea to change a single digit in the URL (although only users with AT & T accounts would be likely to discover the relevance of the ICC-ID).

Auernheimer, who perhaps best can be described as a somewhat infamous self-described troll and grey hat hacker[848], was approached by Spitler online, who shared his discovery with Auernheimer. Auernheimer then assisted Spitler in refining a program called "account slurper". The "account slurper" was designed to automatically change the ICC-ID in the URL and collect the email addresses that appeared on the website.[849] Auernheimer notified the media of the vulnerability, who in turn notified AT & T. After AT & T fixed the vulnerability, the online magazine Gawker showed

---

[845] *US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.)), at 1

[846] Note that changing the browser's user-agent string is by no means a malicious act. User-agent strings allow web servers for example, to deliver requested content optimized for the browser. Furthermore, some browsers identify themselves as many other browsers even though they are not in fact *that* browser. See also note 134.

[847] *US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.)), at *1-2

[848] Generally, there are said to be three categories of hackers; the black hat, who finds and exploits vulnerabilities for his own personal gain or simply out of malice; the white hat, is an ethical hacker who advises companies quietly about discovered vulnerabilities, and might work for security companies and perform penetration tests etc as a part of a contractual agreement; the grey hat, who is somewhat of a mix of a black hat and a white hat, but rarely or never exploits the vulnerabilities for their own gain or out of malice – however the grey hat might inform not only the company but also the public, including hacker communities and let things run their course. *See generally* the Wikipedia article on Hackers for a rough description of the categories. https://en.wikipedia.org/wiki/Black_hat_%28computer_security%29

[849] Just like Phillips' Java program would change the SSN by incrementing the SSN by one each time.

interest in publishing a story on the incident. In order to prove the veracity of his story, Auernheimer shared the list of email addresses with the reporter. Subsequently, a Gawker article detailing the vulnerability and a few redacted email addresses and ICC-IDs were published.[850] AT & T apparently never pressed charges, but the FBI took an interest in the incident and began investigating.[851]

The district court's decision in Auernheimer is particularly interesting for a few reasons. First, the district court, in effect, deemed the access to a publicly accessible website "unauthorized". It did so partially because the access was not gained via the physical device AT&T expected to be used, but via a browser identifying itself as the expected device; something, which is very common although the average user may not be aware of this behind-the-scenes activity or make any changes to the default settings.[852] Moreover, the court did so partially because the court seemingly accepted the government's theory that the ICC-ID numbers were for all intents and purposes "passwords". That is, the government claimed that the ICC-ID was "secret" despite the fact that the ICC-ID was, and still is, an open, documented, publicly available standard[853]; and therefore neither "proprietary" nor actually "secret", which is without doubt the fundamental attribute of a password, because without secrecy the password inherently has no value. Also, the ICC-ID was clearly displayed in the URL itself. The fact of the matter is that the website was accessed in a *manner* that was unintended, by an unexpected person, and the information revealed on the website was unintentionally publicly accessible. Both these elements were used to infer that the access must thus have been unauthorized.[854] In *Auernheimer* the accessibility of the information was unexpected in the sense

---

[850] *US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.)), at *2

[851] http://www.livescience.com/25020-ipad-hacker-guilty-security-research.html

[852] A user-agent-string is sent from the device to the web server telling it what kind of user-agent and operating system the device is using. This string is commonly and easily changed in order to, eg, optimize the displaying of websites in a browser not fully compatible with a website. *See* US v. Auernheimer, Brief of amici curiae Mozilla Foundation et al., p. 7-8. *If you own an Android device, try visiting* whatsmyuseragent.com *(accessed June 23rd 2014) and notice how your device sends a user-agent-string that includes Safari, Mozilla and Chrome even though you are using the Chrome browser*. This is done because web servers sometimes deny sending all or part of the webpage content to browsers that have been deemed incompatible by the administrators of the web server.

[853] ISO standard: ISO/IEC 7812 available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39698 accessed June 23rd 2014

[854] It was extensively argued in amici curiae briefs by the Mozilla Foundation, computer scientists and others, handed in to support the defendant's appeal, that constituting access to such unintentionally accessible information would be detrimental to the IT security research community, since most of the research conducted both implements automated tools to alter URLs as the defendant had done, as well as not explicitly asking the website owner's permission when locating publicly available information that is not intended to be publicly available, nor asking themselves whether the owner would consent to such access, because it is clear that the owner would not consent to exposure of critical vulnerabilities that have gone unfixed or negligently created and thus leaking eg customer information. It would first of all mean that the vulnerabilities would have to be fixed (incurring a cost) and also that the owner's reputation might be

that the owner had at least hoped that only customers accessed the server, and the government argued that the access to the webserver was unauthorized because Auernheimer and Spitler changed the "user-agent" of their web browser, so that when the web browser communicated with the webserver, it would report to the webserver that it was a Safari browser running on an iPad, even though it was in fact a different browser running on a different system. The government's theory was, essentially, that the server, which would only accept connections from browsers running on an iPad, was a server to which access was restricted. However, user-agents are completely within the user's control; it is a setting in the web browser, and as explained above, many web browsers "pretend" to be something they are not, i.e. "lie" about what they are. Internet Explorer "pretends" to be a Mozilla Firefox browser.[855] Almost all web browsers "lie" in that sense by default, and the user can freely change the user-agent through browser settings if they so desire. For example, a person may, for whatever reason, want to load the mobile version of websites by default (where such versions exist) on a desktop computer instead of the desktop versions. This can be accomplished by changing the user-agent of the browser. It is not an access control mechanism; it is an issue of web browser and website compatibility. The question is whether the fact that a server that only accepts connections from computers or devices with certain settings is a fact that makes it justifiable to expect a user to be on notice that access with any other device is unauthorized. However, such an expectation would be highly dependent on a website owner's subjective hopes and wishes with respect to the function, of e.g. user-agents, that are outside the norm or are not realistic.

Auernheimer's trial initially[856] culminated in a guilty verdict and a 41-month prison sentence, even though the "account slurper" program's functions are common practice in the world of IT security

---

damaged. However, justifying keeping vulnerabilities in place to avoid immediate costs related to fixing them, hoping that no one will know, and condemning the persons who may report on the vulnerability to the public, is unlikely to be productive in the long run, since odds are that "worse" people have already found the vulnerability. Regardless of the owner's motive to keep damaging vulnerabilities quiet, this is not an argument to simply start excusing criminal behavior because there was also a benefit to the community involved, but rather an argument, the one discussed earlier, for a paradigm where publicly accessible information is "free" and consent therefore plays no role. It not only alleviates the burden (that of being subject to arbitrary, anti-competitive, unfair terms changeable at the whim of the owner) put on users under the property paradigm, but also places the responsibility where it is most suitable, namely with the owner who is best equipped to introduce security measures to prevent accidental exposure via public accessibility.

[855] Microsoft explains that Internet Explorer identifies itself as Mozilla Firefox for historical reasons. See article at https://msdn.microsoft.com/en-us/library/ms537503%28v=vs.85%29.aspx. Last visited on 5 July 2015.

[856] Auernheimer's conviction was vacated on appeal due to improper forum in New Jersey. The interpretation of the CFAA was not broached by the court, except for perhaps a few comments in dicta. *See US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.))

research, and are no more than automated ordinary user behavior[857], similar to the automated browsing in *Explorica*. Although Auernheimer's conviction was eventually vacated by the Third Circuit, it was vacated because the venue was improper. However, the Third Circuit did say in dicta that "[t]he account slurper simply accessed the publicly facing portion of the login screen and scraped information that AT & T unintentionally published."[858] This, at least, indicates that the Third Circuit did not consider the URLs to be passwords and that no unauthorized access had occurred, even though it did not rule on the issue as such.

Cases like *Auernheimer* provoke a debate that has arguments with merits on both sides. It would be clear to most people that the information accessed by Spitler was not intended to be publicly accessible, even though it was accessible. However, regardless of whether the information was or was not *intended* to be publicly accessible, the server was configured to be publicly accessible, even though only AT & T account holders could proceed beyond the login page. The owner just did not realize to how much information it had given access. However, determining on the basis of the information itself whether access to it is unauthorized or not, presupposes either knowledge that the certain resources on the web server are restricted from public access, even though they are technically publicly accessible, or alternatively, that the information has already been accessed by mistake and suspected to be unintentionally accessible based on appearance or substance. The question is whether a user's mere suspicion of a website owner's lack of intent as to the accessibility of the information is enough to make an accessing user criminally liable. One would hope not.

When comparing *Phillips* and *Auernheimer* the facts are strikingly similar.[859] The only apparent difference – a difference that is meaningless from a technical perspective – is that Phillips' Java program operated by sending requests to the server using a number based on a publicly available formula into a *field on the webpage* whilst Auernheimer's program sent requests to the server *through the URL* where the value was also based on a number derived from a publicly available

---

[857] *See* the above quote from the brief amici curiae filed in support of the defendant-appellant and reversal. Furthermore, it should be noted that anyone with minimal programming knowledge could write a script like the one in question. Even one of the first and easier tasks in the *Python Challenge* (www.pythonchallenge.com accessed June 23rd 2014) incorporates writing such a script similarly aimed at changing parts of URLs automatically and retrieving information from the automatically retrieved webpages.

[858] Discussing whether the access was unauthorized under New Jersey law which requires circumventing code or –password based barrier to access. *US v. Auernheimer*, 2014 WL 1395670 (C.A.3 (N.J.)), at FN5

[859] Phillips' program did cause UT systems to crash several times, but that in itself has no bearing on whether his access was authorized or not.

standard. Technically, whether the request is submitted through a field on the webpage or more directly through the URL is inconsequential from a technical "code" aspect. The difference lies in our perception of what happened and what the defendants could access. Whereas Phillips' action could be seen as "entering" the system, because the SSN was used as a "password" that gave access to all information on the person in the database, Auernheimer's actions did not allow him to gain control of any user's account, because the ICC-ID and the email associated with it, did not actually give him access to the user's account. An "actual" password was needed, in addition to the email address, to move beyond the login page; the manipulation of the URL merely changed the information displayed on the login page. Yet, Auernheimer clearly obtained information from a database in a way not expected by AT & T. The cases appear to differ on another point though, which is, however, inconsequential with respect to determination of guilt under an unauthorized access statute; Auernheimer did not exploit the information he obtained, but notified the media. Granted he could have notified AT & T directly, and he could have refrained from displaying his apparent sense of "schadenfreude"; but what Auernheimer did afterwards has no bearing on whether the actual access was unauthorized. Phillips claimed that he did not intend to exploit or misuse the information he obtained, but he did not notify UT of the vulnerability, either; even though, arguably, the vulnerability inherent in requiring only the entering of a social security number to gain access, is so self-evident that UT probably knew about it, but chose not to invest in better security at that time. Again, what Phillips did afterwards has no bearing on determination of guilt under an unauthorized access statute.

It can be said that whilst Phillips stepped inside the security perimeter and masqueraded as a specific legitimate user, Auernheimer can be said to have stayed at its border and the information he obtained from the login page did not allow him to step inside the security perimeter in such a way that he could masquerade as a legitimate user in a meaningful way. However, the AT & T login page customized the content on it, that is, it pre-populated a field dependent on the ICC-ID provided by a device in the URL, and the ICC-ID was unique to a SIM-card, which in turn was linked to a specific person's email address. Then it can also be said that Auernheimer masqueraded as a specific legitimate user. Auernheimer was never meant to see the email addresses, just like Phillips was never meant to see the information that entering a valid SSN in a login field would yield.

The point is that what appear to be factual differences are not actually factual differences. They are differences in perception. The prosecution is bound to adopt the perspective that argues in favor of guilt, whilst the defendant is bound to adopt the perspective that argues in favor of acquittal. It

raises the question whether the Fifth Circuit would have viewed Phillips' access authorization differently had he entered the SSNs in the URL rather than the login field on the webpage. Something else is happening in these cases other than a pure code-based approach, and it appears to relate to a common understanding of what constitutes a password and a common understanding that use of a password not belonging to you is not authorized. There are no such common understandings with respect to URLs. That is, the norms attached to passwords make it clear that Phillips' access was unauthorized. There are no norms attached to URLs (insofar as they are just used as resource locators, and not to pass malicious code), so it is far less than clear that Auernheimer necessarily did anything wrong; but by using a code-based approach – which at first glance appears reasonable – one can argue that any technical restriction is an access restriction and any value in the URL is password-like because there is no social norm to say otherwise. Code is not irrelevant, but code requires interpreting for its function to be understood, and in this context it is important that it is irrelevant how an owner subjectively intended a program to be used (i.e. for what specific purposes). What is relevant is what the program was designed to do and whether the defendant used the program according to its intended function.

However, there are also cases where the unintended code-based accessibility occurs, not due to the owner's mistake, malfunction in, or lack of, security, but due to accessibility via a third party with a copy of the information.

In *Healthcare Advocates v Harding*[860], a district court decision, a server malfunction caused images to be accessible that previously had been removed from the website, but the server malfunction occurred not with Healthcare Advocates, but with the Internet Archive that hosts the Wayback Machine[861]. The Wayback Machine allows its users to view a website the way it looked at some point in the past. The Internet Archive had designed the crawlers only to make publicly accessible the pages that were not subject to requests set forth in a file called "robots.txt". Therefore, a website owner could prevent the public from viewing (via the Wayback Machine) select pages the way they looked in the past. Healthcare Advocates' webserver supplied such instructions to visiting crawlers. However, when Harding, a law firm involved in litigation against Healthcare Advocates, accessed the screenshots of Healthcare Advocates' website via the Wayback Machine, the Internet Archive

[860] *Healthcare Advocates v. Harding*, 497 F. Supp. 2d. 627 (E.D. Pa. 2007)
[861] Internet Archive https://archive.org/web/ accessed June 23rd 2014

servers were malfunctioning that day and allowed public access to all screenshots regardless of the robot protocol. In this case, the judge concluded that Harding could not be held liable for "luck".[862]

Was Phillips lucky when he managed to retrieve information from TXClass? Were Auernheimer and Spitler lucky when they discovered the association between ICC-IDs and email addresses on AT & T's login page? What seems to matter is not so much supposed code barriers, or their circumvention, but whether it was in a publicly accessible space or closed space, the context in which it occurs and the manner in which the alleged circumvention takes place. In *Morris*, *Phillips*, *Auernheimer* and *Harding*, the accessibility was unexpected and undesired by the owners or right holders. Morris and Phillips were convicted, but Auernheimer's conviction was vacated (although the matter of authorization was only addressed in dicta) and the claim against Harding was dismissed.

So far, it appears that code cannot stand alone.

11.5.1.2 Expected but undesired access

Whereas the accessibility in the above cases was unexpected, code restrictions and their violation also matter in cases where the defendant has been blocked from accessing a website that is available to everyone else but him; that is, access to publicly accessible websites and services.

One such case is *Craigslist v. 3Taps*[863] where the plaintiff had selectively excluded the defendant from accessing Craigslist's otherwise public website.

Craigslist is an American online service provider that through its publicly accessible website allows users to browse classified advertisements posted by other users. 3Taps is a company that offers an API[864] to Craigslist in order for its users to access data in bulk. 3Taps also maintains the website craiggers.com that essentially replicates craigslist.com. To achieve this, 3Taps automatically copies posts from craigslist.com in real-time; that is, 3Taps scrapes the Craigslist website. In order to stop 3Taps undesired use of the website, Craigslist sent a cease-and-desist letter to 3Taps in which it essentially revoked 3Taps' (implicitly granted) authorization to access craiglist.com for any

[862] One could argue that this is because Harding did not use the Wayback Machine contrary to its intended function (reference to the intended function test developed by the 1st Circuit in US v. Morris (1991)) and the access to the Wayback machine was therefore not unauthorized and the defendant never accessed the plaintiff's computers.
[863] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D. Cal. 2013)
[864] Application Programming Interface. Allows third parties to design software that can interact with e.g. a database.

purposes. Furthermore, Craigslist also blocked access from IP-addresses belonging to 3Taps. In order to continue accessing craigslist.com, 3Taps acquired new IP-addresses and used proxy servers with non-blocked IP-addresses, and continued scraping the website.[865]

The case thus revolved around the question whether the owner of a publicly available website could selectively exclude a person; that is, whether the implicit authorization granted to members of the public to access public websites could be revoked with effect for just a select undesirable.

The court answered in the affirmative, because 3Taps had been put on direct notice that it had no authorization to access Craigslist's website anymore both through a cease-and-desist letter and by way of IP-address blocking. 3Taps' circumvention of the IP-address blocking, which the court stated was a technical barrier, albeit an imperfect one,[866] constituted unauthorized access.[867]

3Taps attempted to defend the legality of its conduct by referencing the public accessibility of the website. When addressing 3Taps' argument that the information was public, the court argued that Congress could have specified, but did not, the information it sought to protect by differentiating between non-public and public information. However, the court firmly concluded that there was no persuasive evidence of such a limitation or differentiation in the legislative history.[868] On this basis, the court concluded that an interpretation of "unauthorized" clearly implies the existence of a proprietor's right to selectively revoke authorization to access public websites on a case-by-case basis even when the website is publicly accessible. It seems to be the court's rationale that the proprietor is the authority that can grant authorization and therefore must also be capable of revoking such authorization; even when the authorization is impliedly granted to the entire world, and the revocation aimed at only one or a few select.

---

[865] Craigslist had previously tried to state a CFAA claim based on 3Taps' alleged violation of Craigslist's "Terms of Use". That attempt failed. See *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D. Cal. 2013) at *2, FN3

[866] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D. Cal. 2013), at *6, FN7

[867] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D. Cal. 2013), at *7

[868] The legislative history, as mentioned above, dates back to 1986; a time where there was no such thing as the World Wide Web or any widespread use of the Internet by the general public. There would have been no reason to formulate such a limitation given the state of the "online environment" in the mid-80s. Even when the CFAA was amended, twice, in the mid-90s Congress may not have foreseen the explosive commercial growth of the Internet following the introduction of the web and the subsequent allowing of commercial use of the web. Hence it is rather peculiar to reject an argument like 3Taps' "public versus non-public websites" argument, and accept an argument for the opposite, simply by citing the absence of Congress' discussion of public versus non-public information available. That is, the absence of distinguishing between the two does not equate proof that the legislator intended for there not to be a distinction – the legislator has simply not addressed it, because at the time there was no obvious reason to do so. The court therefore declines the invitation to interpret "authorization" with respect to the significant changes the widespread use of the Internet and emergence of the web has effected in society.

It is worth noting that Craigslist does not mind people accessing the information on craigslist.com, as such; it does, however, mind why the website is accessed, that is, how the information is used subsequently. As several courts have noted so far, including the Ninth Circuit in *Nosal* (discussed above in the section on use vs. access), the CFAA does not prohibit unauthorized use of information; it prohibits unauthorized access to information and computers. However, it is imperative to note that Craigslist was strategic enough to revoke directly 3Taps' authorization to access the website in its entirety, for any purpose. The question of *why* the authorization was revoked becomes immaterial as a matter of law, because as the Ninth Circuit has interpreted the CFAA, the CFAA does not ask *why* a defendant accessed the site, nor does it ask *why* a plaintiff has revoked the defendant's authorization. Craiglist revocation of authorization strategy allowed the court to distinguish the case from *Nosal*[869], a Ninth Circuit precedent that otherwise would have essentially prevented the Craigslist court from considering terms of service or use involving use restrictions disguised as access restrictions. Remember, Craigslist had already tried to rely on its website's Terms of Use in order to get an injunction before it progressed to direct revocation as a basis for getting the injunction.

Although the *Craigslist* court has, from a strict legal point of view, distinguished the *Craigslist* case from *Nosal*, the distinction lies "only" in the blocking of IP-addresses and a cease-and-desist letter. In other words, although the case was correctly distinguished from *Nosal*, *per se*, it perhaps finalized the formation of a whole new trial strategy that allows plaintiffs in cases that involve public websites to "circumvent" *Nosal* altogether, since it can be clearly inferred from *Craigslist* that even though the de-authorization is motivated by and based solely on use restrictions, this cannot be questioned by the courts as long as the plaintiff is not relying on terms of service or use, but instead relies on a direct notification of revocation sent to the defendant. Although this may prima facie strike one as an important difference, the blocking of IP-addresses and the cease-and-desist letter are just different means (as opposed to citing use restrictions disguised as de-authorizations and generally banning competitors from visiting through such terms) to achieve the exact same effect as a general ban on competitors' visits to or use of the website, or any other visits or use by unwanted visitors. In other words, the notice issues may have been addressed, but the breadth issue has certainly not because the owner is free to revoke authorization for any reason, at any time – and perhaps that is a matter for Congress to address rather than the courts, as long as the

[869] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D.Cal.) at *5

courts will not depart from relying solely on a website owner's consent as a source for authorization[870] with or absent symbolic technical barriers.

The Craigslist court chose to interpret "without authorization" in accordance with a trespass analogy/property paradigm, albeit acknowledging it is imperfect, also recognized the problematic breadth of the statute. The court recognized the implications this may have for "innovation, competition and general "openness" of the internet"[871], but concluded that this was a matter of policy for Congress to resolve.[872]

In *US v. Lowson*[873], a case that predates *Craigslist v. 3Taps* but further shows that contract and code is inextricably linked in some cases, the government proceeded to prosecute individuals who had become subject to an investigation after Ticketmaster had failed to state a CFAA claim against a software developer (Ticketmaster had not shown damage or loss as required to maintain a civil action).[874] The defendants had, through the use of software, automated purchases of large blocks of event tickets on the website of the ticket vendor, Ticketmaster, and the defendants then resold the tickets at a profit. Ticketmaster had implemented CAPTCHA ("Completely Automated Public Turing Test to Tell Computers and Humans Apart") on the website and written in its terms that use of the website for commercial purposes was prohibited, as well as prohibiting access by bots. The government's theory was that the defendants had circumvented a security measure which rendered the defendants' access to the website unauthorized. Additionally, the defendants had received cease-and-desist letters from Ticketmaster. The CAPTCHA was not implemented to keep anyone out per se, and thus, did not restrict anyone from accessing the contents of the site; it was implemented to prevent or deter a certain manner of access, that is, automatic access. The crux of the matter is, that CAPTCHA does not protect information from intruders, nor is that its purpose. CAPTCHA's function is to keep out bots, which are typically employed for commercial reasons. The defendants paid the price set by Ticketmaster; they did not steal the tickets because they paid the asked-for price. The government contended that the information obtained by the defendants was "confidential

---

[870] *See* Christine D. Galbraith, 'Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites' (2004) 63 Md. L. Rev. 320-68, 361 et seq. (arguing amongst other things that "[c]ourts evaluating CFAA claims have not limited the manner in which website owners exercise the power to exclude. Although such a power may be a fundamental right of a property owner, it is not absolute." (citations omitted))
[871] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D.Cal.), at *8
[872] *Craigslist v. 3Taps*, 2013 WL 4447520 (N.D.Cal.), at *8
[873] *United States v. Lowson*, 2010 WL 9552416 (D.N.J. 2010)
[874] *Ticketmaster LLC v. RMG Technologies*, 507 F.Supp.2d 1096 (C.D. Cal. 2007)

in the aggregate", ostensibly because repeated accesses to the site's publicly available information made it possible for the defendants to "reveal" a map of available premium seats that normal users would not be able to obtain through normal use.[875] Furthermore, the government argued that the defendants knew their conduct was wrongful because they used numerous non-sequential IP-addresses when purchasing the tickets, which defeated Ticketmaster's IP blocking; the government also alleged that circumventing the IP blocking was a circumvention of code restrictions that made the access unauthorized.

US v. Lowson is a case that exemplifies very well that not only is it difficult to discern which types of code restrictions are actually relevant under an unauthorized access statute, but the case shows that contract and code melt together. The code restriction in *Lowson* was not a restriction that prohibited anyone from accessing the website; the restriction served to weed out those who access the site in an undesirable manner (and in fact weeds out the visually impaired, which CAPTCHA also keeps out in the absence of audio aid). Ticketmaster objected to the how and the why of the defendants' access as stated in their terms, but neither the terms nor the code kept anyone from accessing the website or the information on it. It appears from an amici brief in support of Lowson that Ticketmaster's terms were quite restrictive.[876] The terms for example prohibit anyone from taking notes during events and the terms tie the authorization to access the website to those terms, such that a reviewer/critic attending the concert could be held criminally liable under the CFAA. If Ticketmaster chose to restrict IP addresses belonging to newspapers, bloggers and others who might criticize events or Ticketmaster's services in addition to stating in the terms, as they in fact did, that note-taking was prohibited, should that make the critics criminally liable under an unauthorized access statute? The point is that Ticketmaster wants to remain open to the world and yet closed to those who do not bend to their will; enforced by the threat of criminal law. The defendants may or may not have committed a civil wrong, but enforcing arbitrary terms infused with code through criminal law in a way that would arguably render it illegal for a blind person to use similar software to defeat CAPTCHA in order to buy a concert ticket. If CAPTCHA is a security measure in the sense that defeating it constitutes unauthorized access in *US v. Lowson*, it would equally make a criminal of the blind person; the difference between the actions of Lowson and the blind person lies not in the criminality of the conduct then because both circumvented a code restriction, but rather

[875] See generally *United States v. Lowson*, 2010 WL 9552416 (D.N.J. 2010) at *7
[876] See EFF's amici brief in support of the defendant, p. 20. Available at https://www.eff.org/node/57989. Last visited 5 July 2015.

the difference is merely that the government would hardly pursue a prosecution against a blind person for circumventing CAPTCHA challenges (unless perhaps the blind person became an interesting target for the prosecution for other reasons. See analysis of *US v. Drew* in the next section.[877]).

However, plaintiffs are implementing "code restrictions" that are unrelated to genuine access control, and try to exclude "undesirables" whose conduct may or may not be prohibited by website terms, but somehow offend the owner or whose purposes of accessing a publicly accessible website go against the subjective interests of the owner. They do so whilst keeping the website open to everyone else.

11.5.2 A contract-based approach

This section both analyzes some CFAA claims that have failed as well as those that have succeeded based on contract-related arguments. The purpose of this is to demonstrate the evolution in plaintiff strategy to exclude competitors and other unwanted persons. Although it is called the "contract-based approach", the approach does not solely involve situations where a legally binding contract has been entered into, but rather all cases where the restrictions are based on written terms regarding the use of or access to a computer or information; that is, it appears to be a mix of contracts and what appears to be written expressions of an owner's ostensibly absolute right to exclude others from using their publicly accessible websites and thus computers.[878] A breach of contract may be a separate claim in some cases; however, some courts applying the CFAA in cases where the plaintiff has alleged that authorization was lacking due to violation of Terms of Service or Terms of Use, appear to focus on whether the defendant was on notice regarding the restrictions, regardless of whether the defendant has accepted the terms. The criticism of the contract-based approach has been rooted primarily in that it gives computer owners too much power over the users

[877] The *Lowson* court distinguished *Lowson* from *Drew* stating that the latter did not involve circumvention of code restrictions.

[878] Although *EF v. Explorica* did involve a contract, the contract did not regulate the access to the public website. The case is often counted amongst the cases that follow a contract-based approach. But as has been explained above, and will be explained again to some extent in the chapter on authorization of insiders, there is a distinct and disconcerting disconnect between substance and purpose of the contract and the concept of authorization to access the information on EF's public website. Thus, the case more resembles a kind of social norms approach rather than a contract approach.

of the computers[879] in that the contract-based approach can transform even trivial matters and disagreements into a criminal act at the whim of the owner.

According to a 2013 article on BBC's website, if we were to read the policies related to every website we use, odds are we would have to take an unacceptable amount of time off work; 76 workdays to read all the applicable policies that may affect our authorization to access websites.[880]

Terms of Service, Terms of Use, use policies etc. often describe the rules applicable to the user who is allowed to access and use the service, and these terms are sometimes considered contractually binding upon the user.[881] (Admittedly, the author had – prior to getting acquainted with CFAA case law – always understood such policies and terms to be liability waivers of sorts that would prevent the website owner from being held liable for whatever the user does on the website, or being sued by their users.[882] Orin Kerr expresses a similar understanding in a recent draft essay; that is, that the owner waives liability through those terms and indicate the "right to suspend, block, or otherwise limit access by a user".[883]) Furthermore, it is not uncommon for the service provider to reserve the right to make modifications to the terms without any notice to the user[884], in addition to the user being bound by any additional guidelines posted in relation to the various supplementary/additional services provided by the service provider. In other words, there is an extraordinary amount of reading involved if one wants to be sure not to violate such terms. Acts such as providing false

---

[879] See e.g. Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1651, Katherine Mesenbring Field: Ageny, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819, 847, Patricia L. Bellia: Defending Cyberproperty (2004), NYU Law Review, Vol. 79, p. 2256, and Christine D. Galbraith: Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites (2004), 63 Md. L. Rev. 320, 338

[880] Alex Hudson (bbc.co.uk): Is Small Print in Online Contracts Enforceable? (6 June 2013) at http://www.bbc.com/news/technology-22772321. Last visited on 27 June 2015.

[881] See e.g. *Register.com v. Verio*, 356 F.3d 393 (2nd Cir. 2004) and *Southwest Airlines v. Boardfirst*, 2007 WL 4823761 (N.D.Tex.). NB. Under which conditions these types of terms of service or use agreements are considered valid and binding contracts may vary between Circuits. This article will not attempt to elaborate further upon that subject.

[882] See Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 23. Available at: http://ssrn.com/abstract=2601707

[883] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), pp. 23-24. Available at: http://ssrn.com/abstract=2601707

[884] See for example Yahoo! Terms of Service that state: "By accessing and using the Yahoo Services, you accept and agree to be bound by the terms and provision of the TOS." "Yahoo provides the Yahoo Services (defined below) to you subject to the following Terms of Service ("TOS"), which may be updated by us from time to time without notice to you." --, 'Yahoo Terms of Service' (March 16, 2012) http://info.yahoo.com/legal/us/yahoo/utos/terms/# accessed June 23rd 2014 (US version of the terms) US courts also frequently examine the Terms of Service where the plaintiff/prosecution has alleged violation of 18 USC § 1030. See for example US v. Drew, Koch Industries v. John Does and Cvent v. Eventbrite.

information on the account registration form can result in a "ban" from using the service, as can be seen in the Yahoo! Terms of Service, section 3:

"In consideration of your use of the Yahoo Services, you represent that you are of legal age to form a binding contract and are not a person barred from receiving the Yahoo Services under the laws of the United States or other applicable jurisdiction. You also agree to: (a) provide true, accurate, current and complete information about yourself as prompted by the Yahoo Service's registration form (the "Registration Data") and (b) maintain and promptly update the Registration Data to keep it true, accurate, current and complete. If you provide any information that is untrue, inaccurate, not current or incomplete, or Yahoo has reasonable grounds to suspect that such information is untrue, inaccurate, not current or incomplete, Yahoo has the right to suspend or terminate your account and refuse any and all current or future use of the Yahoo Services (or any portion thereof)."

If such a ban on using the Yahoo services were issued, it would clearly be contrary to the Terms of Service if one would access the service in spite of the ban. The question is whether visiting a website with disregard for such a ban falls within the scope of hacking statutes prohibiting unauthorized access so that a breach of Terms of Service, be it contractually binding or not, becomes a criminal act.

CFAA claims based solely on "de-authorizations" found in website terms of service or use have generally been unsuccessful in US case law. The language of the terms relied on by the plaintiffs have varied; some phrasing their terms to describe "unwanted use" as a "de-authorization" (an approach that has been rejected by most courts), some prohibiting automatic access, e.g. by bots, spiders, scrapers etc., and at least one that just directly in its terms prohibits access to the website by competitors[885].

One of the earliest contract-based cases was *AOL v. LCGM*.[886] AOL, an ISP (Internet Service Provider) provided internet access, chat room services, email services and more to its members. LCGM was an online business that offered pornographic websites. AOL filed a CFAA complaint against LCGM, alleging that LCGM had exceeded its authorized access to AOL computers by using their AOL account to harvest email addresses of other AOL members in adult chat rooms in violation of AOL's Terms of Service. Afterwards, LCGM had sent bulk email to the email addresses that it had obtained; the emails were necessarily routed through AOL's computers to be delivered to AOL member's email inboxes. Sending of bulk email was also in violation of AOL's

[885] *See EF Cultural v. Zefer*, 318 F.3d 58, 63 (1st Cir. 2003) where the First Circuit, in dictum, rejected the notion of such terms because prohibiting competitors would raise serious public policy issues.
[886] *America Online, Inc. v. LCGM, Inc.*, 46 F.Supp.2d 444 (E.D. Vir. 1998)

Terms of Service and AOL's Unsolicited Bulk Email Policy. The *AOL* court did not discuss at any length what authorization means in the context of the CFAA. The court concluded laconically that "[d]efendants' actions violated AOL's Terms of Service, and as such was unauthorized."[887] The court concluded the same with respect to AOL's claim that LCGM violated the CFAA when sending bulk email *through* AOL computers.[888]

Another court went further. In *Register.com v. Verio*[889], Register, a domain name registrar, sued Verio, a website design service for unauthorized access to WHOIS information provided by Register. Register was appointed as a domain name register by ICANN (Internet Corporation for Assigned Names and Numbers). According to Register's contract with ICANN, Register was obligated to, among other things, provide free public access through the Internet to WHOIS information. The ICANN agreement also required that the registrar "not impose terms and conditions on the use made by others of its WHOIS data except as permitted by ICANN-adopted policy"[890]. ICANN had then specified that "[…] the ICANN Agreement requires the registrar to permit use of its WHOIS data "for any lawful purpose except to: … support the transmission of mass unsolicited, commercial advertising or solicitations *via email (spam)* […]"".[891] The ICANN agreement that bound Register, instructed Registrar as to in which way it could restrict the *use* of WHOIS information. Register therefore attached the following terms to the response to each WHOIS query: "By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to … support the transmission of mass unsolicited, commercial advertising or solicitation via email."[892]

Before the district court, Register argued that Verio's method of accessing the WHOIS information and Verio's end use of the WHOIS information violated the CFAA. The district court agreed. Like the district court had held in terms of Register's trespass to chattels claim, the mere fact that Register had objected to Verio's use of robots to retrieve the WHOIS information meant that the access to the information was unauthorized. As also noted by Kerr, this is perhaps one of the

[887] *AOL v. LCGM*, 46 F.Supp.2d 444, 450 (E.D. Vir. 1998)
[888] *AOL v. LCGM*, 46 F.Supp.2d 444, 451 (E.D. Vir. 1998)
[889] *Register v. Verio*, 126 F.Supp.2d 238 (S.D.N.Y. 2000) (CFAA claims were addressed by the district court; the Second Circuit decision, which is also discussed to some extent, addressed appeals regarding trespass to chattels)
[890] *Register v. Verio*, 356 F.3d 393, 396 (2nd Cir. 2004)
[891] *Register v. Verio*, 356 F.3d 393, 396 (2nd Cir. 2004)
[892] *Register v. Verio*, 356 F.3d 393, 396 (2nd Cir. 2004)

broadest readings of the CFAA to date.[893] The fact that Register filed suit against Verio, was Verio's notice that the access was unauthorized under a primarily criminal statute.[894] Furthermore, the court held that even if Register had not prohibited access by robots, Verio's "access would be rendered unauthorized *ab initio* by virtue of the fact that prior to entry Verio [knew] that the data obtained will be later used for an unauthorized purpose."[895] Thus, even though Register was only allowed to restrict the use of the WHOIS information as provided for in its contract with ICANN, Register went beyond those allowed restrictions, and furthermore, managed to convince a court that later unwanted use of data was generally relevant under the CFAA, which regulates access, and to use a primarily criminal statute to enforce these use restrictions that were in violation of their own contract with ICANN.

Because the district court's CFAA reasoning was based on its trespass to chattels reasoning it is worth taking a brief look at what the Second Circuit said about the trespass to chattels claim on appeal. The Second Circuit argued, in terms of trespass to chattels, that because Verio admitted to knowing the terms, and because the terms were attached to the responses to WHOIS queries[896], the court held that Verio had assented to the terms, describing it through an apple stand analogy. The court argued, in regards to terms of use, that when walking up to a stand where apples are sold, one cannot simply take an apple and not pay for it just because one has not read the price sign or chooses to ignore it. This is a rather odd and fundamentally inaccurate analogy that serves to further a misplaced argument that confusing the terms "use" and "access". There is a fundamental difference between goods that are taken because they are free and goods that are for sale but are taken without payment. Let us say for instance that the apple stand sign stated that the apples were free, but you could only take some if you took at least two and also you would have to share the other apple with another person in your household. One could more validly argue that since the

---

[893] Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, p. 1639

[894] As mentioned before, but bears repeating because of its importance; even though *Register v. Verio* is a civil case, the CFAA is primarily a criminal statute and, as such, judicial interpretations of the statute in civil cases also apply in criminal cases. It is for this exact reason that the courts should be observant of the rule of lenity even in civil cases under the CFAA. Broad readings that may be tentatively acceptable under civil statutes due to the less strict notice (foreseeability) requirements are not acceptable where such broad readings must also be applied in criminal cases because the civil case interpretation flows into the criminal cases where the notice (foreseeability) requirements are much stricter. Especially so when the statute is of general applicability; that is, the regulated are the population at large and not a specifically targeted group, for example a certain industry or business sector that could effect a less strict notice requirement.

[895] *Register v. Verio*, 126 F.Supp.2d 238, 253 (S.D.N.Y. 2000)

[896] *Register v. Verio*, 356 F.3d 393, 397 (2nd Cir. 2004)

apples were free and made accessible to the public, the best the stand owner could achieve is the *hope* that people would do as the sign suggested, but he has in fact effectively relinquished any proprietary right and ability to state any terms regarding the use of the apples and enforce such terms. Equally, the owner could not require a person to consume the apples raw in his home and not bake an apple pie at his grandmother's house. The owner would have no claim as to the subsequent use of the apples, but only insofar as he limits the number of apples that are free per customer (meaning that for example, only the first three apples are free and payment is expected for any apples taken subsequent to that). For the same reasons, a website owner should not be able to enforce restriction on the *use* of information publicly available for free on websites through an *access* provision. Therefore, he cannot *turn* the *access* unauthorized just because the information was not *used* in the way the owner wanted, nor could he claim that using the information in an unwanted way (e.g. for an unwanted purpose) was exceeding authorized access; at least not under a 'hacking' provision that prohibits unauthorized access; but maybe more appropriately under e.g. copyright laws insofar as the information is protected by such laws.[897]

In *Southwest v. Farechase*[898], the plaintiff, the low-fare airline Southwest, filed a CFAA unauthorized access claim against Outtask and Farechase, a software company that licensed scraping software to Outtask, who in turn used the Farechase software in a software product that allowed corporate travelers to search for air fares. Since Farechase's software scraped information from Southwest's website in violation of the website's use agreement, Southwest claimed that Farechase and Outtask had accessed the website without information in violation of the CFAA.[899] Although Outtask argued that the use agreement did not constitute a contract, the court stated that "[r]egardless of whether the Use Agreement creates an enforceable contract for purposes of a breach of contract claim pursuant to state law, Outtask knew that Southwest prohibited the use of "any deep-link, page-scrape, robot, spider or other automatic device, program, algorithm or

[897] Information could be protected under e.g. copyright laws, trademark laws or data privacy laws if they meet the requirements for such protection. Granting a blanket-protection under hacking statutes for all information would only serve to stretch use-regulation, such as copyright, further than intended by the legislature by granting copyright-like protection to e.g. factual information on websites solely on the basis that the information is accessed on a computer. See further copyright discussion regarding factual information on publicly accessible websites Christine D. Galbraith, 'Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites' (2004) 63 Md. L. Rev. 320-68

[898] *Southwest Airlines v. Farechase*, 318 F.Supp.2d 435 (N.D. Tex. 2004)

[899] Southwest's complaints against Farechase and Outtask consisted of the ostensibly normal slew of claims that arguably could perfectly cover any undesirable conduct in absence of CFAA coverage; i.e. misappropriation, breach of contract, interference with business relations, etc.

methodology which does the same things." Southwest had also notified Outtask directly that their access to the website was unauthorized. This is the extent of the court's analysis of authorization; the lack of analysis is reminiscent of *AOL v. LCGM*. Like AOL in *AOL v. LCGM*, it is not the principle of access, as such, that Southwest is concerned with; it is the purposes of the access and purposes of obtaining the information. That is, it is a question of what the defendant is going to do with the information later on and whether that is in the plaintiff's interest.

The same district court decided another case involving Southwest Airlines a few years later in *Southwest v. BoardFirst*[900]. However, since the last Southwest case, the Fifth Circuit had rendered a decision in *Phillips* (discussed above in the section on code-based approach). Southwest again cited a violation of its website's terms of use as a basis for a CFAA violation, in addition to cease-and-desist letters. Southwest's seating policy on the airplanes was based on a "first come first served" basis, such that those first 45 customers who first check in within the first 24 hours before departure get an "A" boarding pass and get to board before other those passengers who get "B" or "C" boarding passes. BoardFirst's reason for being was to serve Southwest customers, for a fee, by logging onto the website for them and get the desirable "A" boarding pass. The customer would supply BoardFirst with the information needed to log onto the website on their behalf. However, the website's terms of use prohibited use of the website for commercial purposes. Southwest later added language to the effect that excluded BoardFirst's practices explicitly, as well as sending cease-and-desist letters to BoardFirst. Therefore Southwest claimed that BoardFirst had violated the terms of use, and thus the CFAA. Although the court found that BoardFirst had breached a contract when it violated the terms of use, the court was hesitant when it came to the question of whether violation of terms of use triggered the application of the CFAA. The court left it an open question, allowing the parties to submit trial briefs on the question of "authorization" in the context of the CFAA, but emphasized that *Zefer*, *Farechase*, *Explorica*, *Register*, and *AOL v. LCGM* had received criticism from commentators. Furthermore, the court cited *Phillips* and the "intended function" test (the objective version), and noted that the defendant had used the website according to its intended *function* regardless of whether the terms of use did not sanction the *purpose* for which BoardFirst used the website (for financial gain); the CFAA prohibits unauthorized access to computers, not using a computer for a prohibited purpose.[901]

---

[900] *Southwest Airlines v. BoardFirst*, 2007 WL 4823761 (N.D. Tex. 2007)
[901] *Southwest Airlines v. BoardFirst*, 2007 WL 4823761 (N.D. Tex. 2007)

What is perhaps one of the more insidious of attempted applications of the CFAA occurred in *US v. Drew*.[902] Recall that although the cases analyzed so far where the basis for the CFAA claim has been a violation of terms have been civil cases, the interpretation of civil cases applies in criminal cases as well, since the CFAA is primarily a criminal statute. Thus, it was arguably inevitable that the government pursued a similar strategy in a criminal case. Lori Drew was found guilty by a jury for a misdemeanor[903] violation of the CFAA based on her having lied about her name, age and gender on MySpace and posting a picture of someone other than herself without that person's consent in violation of MySpace's Terms of Service. Drew had been masquerading as a fictitious 16-year old boy on MySpace. She used the profile to cyberbully a 13-year old girl, Megan, over the course of roughly a month. Megan ended up committing suicide the same day as Drew, pretending to be the 16-year old boy, told her that "the world would be a better place without her in it."[904] Upon learning of Megan's death, Drew deleted the fictitious boy's MySpace profile. The government's theory was that Drew's intentional violation of MySpace's Terms of Service constituted unauthorized access to the service and thus triggered criminal liability under the CFAA. Drew argued that such a construction of the CFAA would render it unconstitutionally vague. The court agreed with Drew and granted her motion for acquittal.

According to the court, the government's theory failed both prongs of the void-for-vagueness doctrine, because (a)(2)(C) would become a law "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[905]

Intentional violation of website terms of service failed the notice requirement for several reasons. (1) A contract breach is normally not subject of criminal prosecutions; especially, so where the service is provided for free, as was the case with MySpace. Ordinary users would not expect criminal prosecution for violating such terms.[906] (2) If terms of service and the likes really control authorization to access and thus control the criminality of any given access, (a)(2)(C) would be void for vagueness, because "it is unclear whether any or all violations of terms of service will render the

[902] *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)
[903] The government had pursued a CFAA felony conviction, but the jury found Drew not guilty on the felony charges (unauthorized access in furtherance of violation of a state law or tort).
[904] *United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009)
[905] *United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (citing *City of Chicago v. Morales*, 527 U.S. at 64, 119 S.Ct. 1849)
[906] *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009)

access unauthorized, or whether only certain ones will."[907] Although stating that any and all violations would be criminal would solve this specific notice problem, doing so would render the statute overbroad and violate the second prong of the void-for-vagueness doctrine (sufficient guidelines to those enforcing the law).[908] (3) Allowing violations of terms of service to form the basis of a CFAA violation delegates to the website owner to define what conduct the CFAA criminalizes, and thus compounds the vagueness problems.[909] (4) Application of contract law and contract clauses invite other problems, such as where a dispute is subject to arbitration (a question of whether the court can make a finding as to authorization when the contract requires resolution of disputes through arbitration). Lastly, the court notes that under California law, a breach of terms of service "does not automatically discharge the contract, but merely "excuses the injured party's performance, and gives him or her the election of certain remedies.""[910]

The second prong of the void-for-vagueness doctrine requires, as may be recalled from the chapter on nullum crimen sine lege, that statute provides sufficient guidelines to those enforcing the law. The *Drew* court stated that the government's theory failed that prong as well. If any violation of terms would incur criminal liability, the range of behavior that would be rendered criminal is infinite. For example, Facebook's terms of service prohibit violating the spirit of the terms.[911] Putting that together with section 3.11 of the terms that essentially prohibits aiding and abetting others in violating any part of the terms or Facebook's other policies, there is no limit to criminal liability. As pointed out by the *Drew* court, prosecutors could pick and choose who to prosecute because lying about your age, weight or other information about yourself would constitute a breach of MySpace's terms. Such staggering breadth in addition to the fact that the prosecution need not await a complaint from the service provider. In both *Drew* and *Auernheimer* the service providers did not file complaints against the defendants. Anything and everything could be prosecuted. The government's theory, given that the statute does not require there be any harm done nor that there has been a violation of privacy interests[912], would result in a "standardless sweep" that would leave "federal law enforcement entities […] improperly free "to pursue their personal predilections.""[913]

---

[907] *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009)
[908] *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009)
[909] *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009)
[910] *United States v. Drew*, 259 F.R.D. 449, 465-466 (C.D. Cal. 2009)
[911] See Facebook's Terms of Service § 14. Available at https://www.facebook.com/legal/terms. Last visited 2 July 2015.
[912] *United States v. Drew*, 259 F.R.D. 449, 466-467 (C.D. Cal. 2009)
[913] *United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (citing *Kolender*, 461 U.S. 358, 103 S.Ct. 1855)

Even though other courts had previously held that breach of terms of service would suffice to trigger liability under the CFAA they had only ever done so in civil cases. As noted by several commentators, the fact that the CFAA has been primarily interpreted in civil contexts is likely the root cause of its current expansive scope, which applies equally in criminal cases. Conduct that violates the CFAA in a civil case is criminal conduct under the CFAA.[914]

In *Cvent v. Eventbrite*[915], Cvent, a company that, among other things, maintained an online database of venues for large events, had written in the website's terms of use that "[n]o competitors or future competitors are permitted access to our site or information, and any such access by third parties is unauthorized…".[916] Eventbrite, a company also in the event planning business, had scraped venue information from the Cvent web-based database, which was publicly accessible via Cvent's website and later posted the information on its own website. Cvent proffered only one argument in support of the CFAA claim; the terms of use prohibiting competitors from accessing the site and information on the site. The court did not comment on the language of the terms, but dismissed Cvent's claim (1) because the terms were difficult to find on the website, and, (2) because Cvent had not taken any affirmative steps to screen competitors from accessing the information.[917] For those reasons the court found that the website and the database were not protected in any meaningful way.[918]

The CFAA does not ask why information was accessed, it just asks whether the access was authorized.

11.5.3 A social norms approach?

The social norms approach has not really been articulated in US case law as an independent approach. The Fifth Circuit in *Phillips* stated that courts typically analyze authorization from the point of "expected norms of intended use or the nature of the relationship established between the computer owner and the user."[919] However, as noted before, the Fifth Circuit followed a subjective

---

[914] See discussion of *United States v. Lowson* above. The case started as a civil case. The government proceeded with criminal prosecutions after the defendants lost the civil case.
[915] *Cvent v. Eventbrite*, 739 F.Supp.2d 927 (E.D. Vir, 2010)
[916] *Cvent v. Eventbrite*, 739 F.Supp.2d 927, 932 (E.D.Vir. 2010)
[917] *Cvent v. Eventbrite*, 739 F.Supp.2d 927, 932 (E.D. Vir. 2010)
[918] The court cited e.g. *LVRC v. Brekka* as support. *Brekka* is analyzed in the chapter on insiders.
[919] *United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007)

approach rather than an objective one as in *Morris*, which it nonetheless cited as support; the Fifth Circuit arguably follows a less "random" approach than the application of a "reasonable expectations test" rejected by the First Circuit in *Explorica*, a test that made even the presence of hyperlinks a sign that a certain manner of access was unauthorized. But as will be shown, a subjective approach is indicative of a lack of a social norm. The CFAA does not provide answers to the question of what authorization means, and thus courts must figure out what that is, and in doing so have hooked into the traditional trespass doctrine, agency law and so on, to find legal arguments for liability where the behavior is socially unacceptable and could under creative theories be squeezed within the concept of unauthorized access even where the objectionable conduct is not related to the principle of the access itself, but rather later use of information gained through an otherwise authorized access. What does "code" mean, anyway? Should terms of service, or contracts unrelated to the access, matter?

It was argued in the section on the code-based approach that there is no technical difference between what Auernheimer did (changed digits in the URL) and what Phillips did (changed the SSN number submitted to a field on the page). In both cases information was extracted that was not meant to be extracted, and code technically allowed both defendants to proceed. In Auernheimer's case one would be hard-pressed to call the value in the URL a password, where the login page requested a password independently of the changed value in the URL. Although Auernheimer was convicted in the district court, his conviction was vacated on appeal due to venue issues. The Third Circuit stated, in dicta, that Auernheimer had only viewed the public facing portion of the website, indicating that it was the court's opinion that Auernheimer had not violated the CFAA. However, Phillips was convicted as well, and his conviction was affirmed by the Fifth Circuit. But in Phillips' case, the webpage made the entering of a social security number fit our collective perception of a password, regardless of how inherently insecure this technical barrier was due to the authentication being based only on supplying an SSN and nothing else. Furthermore, Auernheimer never attempted to proceed beyond what is perceived as the security perimeter (he remained on the login screen), whereas Phillips did proceed beyond what is perceived as the security perimeter, regardless of its efficacy.

If there is no real technical difference, then the differences must lie elsewhere. Of course there is the possibility that the Fifth and Third Circuits simply disagree on the matter. It is more likely, however, especially granted the Fifth Circuits references to *Morris*' "intended function" test (although the Fifth Circuit gives the Second Circuit's test a subjective spin) and the district court's

"reasonable expectations" test in *EF v. Explorica*, that the Fifth Circuit was relying on how people perceive password prompts on webpages and what password prompts are intended for. The Fifth Circuit's reference to the rejected "reasonable expectations" test is perhaps a bit misplaced, because the district court went too far in the *Explorica* case by arguing that the presence of hyperlinks and dropdown menus indicated a restriction on how information may be accessed that is otherwise publicly accessible, and that the copyright symbol meant that there could be restrictions on use of information that was not actually capable of being protected by copyright law. However, the Fifth Circuit was right on the money in terms of people understanding what a password prompt represents. Everyone inherently knows that guessing passwords is wrong – at least when it is not your own account to which you have simply forgotten your password. The question is, should that affect how other cases are decided that do not involve passwords, where the plaintiff simply calls something a "secret" or a "password" without that something being perceived by society as such? Arguably, the answer is no, because where intersubjectivity is lacking – which most certainly was the case in the district court's test in *Explorica* – there is no norm; no common understanding.

The social norms approach does not appear to render code restrictions meaningless. The social norms approach ties directly into code in some cases, such as *Morris*, which will be revisited briefly below.

The problem with the code-based approach is that it does not appropriately solve cases where the machine authorized the access, but the offender clearly knew he had no authorization to access the machine. Peter Winn used an Australian case to exemplify such a situation.[920] In the Australian case, the defendant had opened a bank account and gotten a bank card so he could withdraw money from his account from ATMs. The ATMs were setup in such a way that when an ATM was "online" it would check the available funds in the customer's account. However, when it was "offline" an ATM would allow the customer to withdraw up to $200, without checking whether there were sufficient funds in the account. The defendant had closed his account and then used his bank card to withdraw money from an "offline" ATM. Of course, anyone knows that if you have no account with the bank anymore, then withdrawing money from an "offline" ATM using the old bank card is clearly not authorized, regardless of whether the ATM allows the withdrawal or not.

[920] Peter A. Winn: The Guilty Eye: Unauthorized Access, Trespass and Privacy (2007), 62 Bus. Law. 1395, 1407

The Australian High Court made a point out of noting that the machine cannot give consent on behalf of the bank where the customer has no account with the bank.[921]

For those advocating a pure code-based approach, the approach will break down, because code means something to us in some contexts and something else or nothing specific in others contexts. For example, if we compare the Australian ATM case with *Auernheimer*; the ATM allowed the withdrawal to occur even though the authorization to withdraw from the bank account cannot persist beyond the closing of the account, whereas the AT & T servers allowed Auernheimer and Spitler to extract information that AT & T would not have allowed them to extract had they been asked. Both the defendant in the Australian case and Auernheimer and Spitler exploited perceived vulnerabilities. Then why is the Australian defendant so clearly culpable whilst Auernheimer and Spitler are less so?

There are several possible answers. One answer could be that the Australian defendant caused harm in that the bank sustained a monetary loss; he took money that he knew did not belong to him. A second answer, which includes the former, could be social norms. The involvement of the concept of authorization in the Australian case seems to stem from the defendant's analogy to Australian common law. The defendant would not have incurred liability had a bank teller mistakenly given him the $200 because they did not know the defendant did not have an account with the bank anymore. Then why would the defendant incur liability when the same mistake is made by a machine? The Australian court answered that a machine cannot consent to anything. That is, the Australian High Court stated that only a human being can give consent. Peter Winn then argues on the basis of the Australian case that what machines authorize or allow has no bearing on whether there is authorization to access a computer.[922]

However, Winn's argument does not sound reasonable or practical either, because code and the perception of the code's purpose affects how the user perceives authorization. Those arguing in favor of a pure code-based approach and those more inclined to accept Winn's approach that favors a person's consent regardless of code arguably under- and overcriminalize (depending on a narrow or broad understanding of code restrictions) and overcriminalize, respectively. A code-based

[921] See summary of *Kennison v. Daire* in Peter A. Winn: The Guilty Eye: Unauthorized Access, Trespass and Privacy (2007), 62 Bus. Law. 1395, 1407

[922] Peter A. Winn: The Guilty Eye: Unauthorized Access, Trespass and Privacy (2007), 62 Bus. Law. 1395, 1408. In agreement with Winn is Matthew Kapitanyan: Beyond WarGames: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context (2012), 7 I/S: J. L. & Pol'y for Info. Soc'y 405

approach would let the Australian defendant off the hook for withdrawing money he knew he was not authorized to withdraw. Winn's approach would be highly problematic in cases like *Auernheimer* involving the web where access to public websites is implicitly authorized because the servers allow access to the websites subject to the owner's server setup but where the owner failed to foresee the way the server would leak information or how it would be accessed and could thus not have agreed to an unexpected scenario. Auernheimer and Spitler knew that AT & T did not intend to make the email addresses publicly accessible, but AT & T left the information in a public space outside the "perimeter" so to speak.

Perhaps the answer to the question regarding culpability is a mix of social norms, code and harm. Where harm is caused, we usually find it socially unacceptable, whereas where no harm was caused because the defendants did not maliciously exploit what they obtained, we are more forgiving. The point is merely that code and owner consent are interlinked; in some contexts we may think it fair to let code be decisive and in others let the owner's consent be decisive. Code-based approaches are arbitrary if applied broadly without regard for the objective intended function of the code. Code is often reusable in various contexts, but password prompts we understand as access restrictions, whereas hyperlinks we do not understand to be access restrictions regardless of whether a website owner may construe them that way on his website. We can similarly agree that for the rest of this dissertation the word "fork" refers to a "knife" and we agree to use knives as forks, but our new shared understanding of the word "fork" and the redefined common understanding of how one uses a knife, has no bearing on how the world around us understands the word and how they choose to use cutlery. The code-based approach is, or can be, arbitrary without an interpretation of what the code is meant to do and not what a specific owner wanted to use the code to accomplish. The code could be interpreted more or less objectively and it could be interpreted subjectively; more objectively, as in the Second Circuit's "intended function" test, or subjectively, as in the Fifth Circuit's more subjective version, the "intended use" test. The Second Circuit did not ask what the specific computer owners how they intended the programs to be used, but what the program's intended *function* was. The Fifth Circuit, however, focused on how the University of Texas subjectively intended their computers and networks to be *used* in light of a computer use policy in order to find that conducting port scanning constituted unauthorized access because port scanning did not comport with the university's intended use of the computers and networks.

Professor Kerr has very recently published a draft of a forthcoming essay called "Norms of Computer Trespass". As may be recalled, it was Kerr who argued that authorization could be

analyzed from two approaches, which he divided into code-based and contract-based. At the time of his 2003 article that described this distinction there existed some case law that supported such a distinction, and at the time it was also clear that the uncertainty and vagueness imposed by the contract-based approach made the narrower code-based approach more reasonable. However, as will become clear, especially in the light of the below chapter on insiders, the code-based approach does not and never has been capable of providing a comprehensive framework for analyzing authorization; it has its faults. The approach fails to cover e.g. a random visitor's or a janitor's unauthorized access to an unprotected computer, because code did not prevent them from accessing the computer, and thus, under a strict application of the code-based approach they would be authorized to access the computer. But such a conclusion is immediately recognizable as being erroneous, because it goes against our social norms. We all know that when we go to a store, we cannot go to an employee's computer and start using it to check inventory or payroll just because there was no meaningful code-based restriction to keep us out. Lack of authorization is obvious in this particular context.

11.5.3.1 Social norms dimensions of trespass

Kerr has recognized in his draft essay that the code-based approach he favored fails to appropriately address access that is clearly unauthorized based on clear social norms, and furthermore, that the code-based restrictions are hard to separate from the contract-based restrictions in some cases,[923] since code and contract may be more interlinked than previously anticipated. Kerr then argues in favor of a social norms approach to analyzing authorization that appears to be based on the Second Circuit's analysis in *Morris* as well as using traditional trespass theories as a doctrinal hook.

Kerr's amended proposal for analyzing authorization focuses on social norms associated with traditional trespass concepts; the social norms associated with (1) the nature of the space, (2) the means of access, and (3) the context of the access.[924]

(1) The nature of space is inherently linked to our perceptions of "perimeters". The walls of a residential house indicates a perimeter in physical space. We know from the appearance of that

[923] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 5. Available at: http://ssrn.com/abstract=2601707
[924] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), pp. 8 and 14. Available at: http://ssrn.com/abstract=2601707

house that we are not allowed to enter it unless we have been invited in or specific circumstances indicate that normal rules do not apply, such as a real estate agent's open house.[925] The walls of a supermarket also indicate a perimeter in physical space, but different social norms apply with respect to a supermarket compared to the social norms that apply to residential houses.[926] Supermarkets we can enter – during opening hours – without asking permission or knocking on the door, ringing doorbells or the likes to explicitly illicit our authorization to access. The appearance of the space itself in combination with social norms guide our perception of authorization.

(2) As to the means of access, we know not to enter a house through a window, a chimney, a pet door or entering the house by breaking down the wall. None of these methods of entering a house comport with the "intended function" of a window, chimney, pet door or a wall.[927]

(3) Norms associated with the context of entry are relevant to authorization to entry. As Kerr explains, locks are a form of access control. Only a select few have keys to our personal homes. The lock's function is to keep those out who do not have a key, and let those in who do. But at the same time, if you lose your key and someone finds it, the person finding the key is obviously not entitled to enter your house solely based on possession of the lost key.

However, although the framework of traditional trespass analysis may be useful in a computer context, analogies to social norms governing access to private residences and other buildings or areas are not as transferrable because the nature of the space is quite different.

Kerr points out that without experience with the norms, a person observing the norms from the outside may perceive the social norms as arbitrary rules.[928] Although judges may be as familiar as any other person with the social norms that control the authorization to enter physical spaces, they are not necessarily familiar with computers or common practice in the computer context. Peter Winn, for examples, appears to reject any notion suggesting that "computer nerds" should dictate

---

[925] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 8. Available at: http://ssrn.com/abstract=2601707
[926] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 8. Available at: http://ssrn.com/abstract=2601707
[927] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 11. Available at: http://ssrn.com/abstract=2601707
[928] Using as an example a Martian visiting Earth for the first time and finding social norms confusing and arbitrary, because he is not familiar with the signals and the rules those signals indicate to those with experience. See Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 6. Available at: http://ssrn.com/abstract=2601707

norms in a computer context.[929] However, those "computer nerds" are those that are most familiar with existing norms and those most in touch with ongoing developments and practices. To judges any given conduct may appear entirely alien even though it is a norm in the context of computers and networks. If judges know enough about the technology and how it is used they are better equipped to recognize norms,[930] and will thus also be better equipped to reject suggested or developing norms that are undesirable or harmful.

Kerr cites *Morris* as an example of a case that incorporates the three questions of network access: the nature of the space, the means of the access and the context of the access. Nature of the space: Morris' conduct took place in a pre-web environment where access to a machine was password-controlled. Access was not open, but dependent on the user having an account on the computer.[931] Means of access: Morris exploited vulnerabilities in the finger daemon and the SEND MAIL program (he used the programs against their "intended function") and gained "special access".[932] As discussed before, in the section on code-based approach, the Second Circuit's "intended function" test relies on a more objective perspective rather than subjective; this is further emphasized by Kerr, who points out that it is important to point out that "the difference between bug and feature boils down to social norms rather than subjective intent."[933] If the means of gaining access is a feature it points towards the access being authorized, whereas if the means of gaining access is exploitation of a bug it points towards the access being unauthorized. Finally, the context of the entry: Morris' worm guessed passwords. As also pointed out earlier in the section on the code-based approach in connection with *US v. Phillips*, entering a password into a password field is the exact intended function of that field. Whether the password turns out to be ill-gotten and the person using it is not the person authorized to access is immaterial to the "intended function" of a password prompt. However, it flows from the context of the access (i.e. the person is using a password not belonging to them) that the person is unauthorized to use that password. Authorization to access has not been

[929] See Peter A. Winn: The Guilty Eye: Unauthorized Access, Trespass and Privacy (2007), p. 1434
[930] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 14. Available at: http://ssrn.com/abstract=2601707
[931] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 17. Available at: http://ssrn.com/abstract=2601707
[932] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 17. Available at: http://ssrn.com/abstract=2601707
[933] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 18. Available at: http://ssrn.com/abstract=2601707

delegated to the person illegitimately using the otherwise valid password.[934] It goes against social norms to guess other people's passwords. This would apply regardless of whether one favors a strict code-based theory that asks whether code prohibited the entry or whether one favors a contract-based theory where the terms of service prohibit guessing other people's passwords. No code or contract needs to tell us that password-guessing is wrong; we know from experience. It is perhaps one of the clearest examples of unauthorized access and the use of other people's passwords to obtain information from a computer that one is not entitled to obtain is specifically mentioned as an example in both the Danish and US legislative history.

In order to figure out whether accessing a computer is authorized it is important to understand the nature of the space. With respect to computers, the space can be physical in the sense that a janitor may have physical access to a computer because he is allowed to do maintenance in the room where the computer is located, or a library computer that is made available to anyone visiting the library. The space can also be virtual; closed networks or services where a person needs to be registered user (i.e. have an account) to be authorized to access, and open networks or services where anyone can freely access some parts of or the entire computer. Open networks and services, such as the internet, the web, public websites on the web, are left open and publicly accessible by default; in there lies the value of the internet and the web – the more people who use these publicly accessible entities, the larger the audience the content and service providers have. However, different services or applications may have different norms[935], because the perception of the space is different; that is, the perception of the perimeter and thus the rules for traversing the perimeter may differ.

Since many of the problems discussed in this thesis relate to the web, an examination of the web is pertinent. The web is a "global computer networked information system."[936] The nature of the space is suggested by the adjective of that quote, namely, "global". Of course, that does not mean that anyone with a webserver has to make its content available to anyone (this is not an advocacy for mandatory open access!), but on the other hand, a person who publishes information on a public website cannot claim that they expected the information to be anything but globally accessible; just like a published author cannot expect that his published book is not publicly accessible, or publish

[934] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 18. Available at: http://ssrn.com/abstract=2601707
[935] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 37. Available at: http://ssrn.com/abstract=2601707
[936] CERN's document releasing the web software into the public domain (30 April 1993). Available on CERN's website at http://tenyears-www.web.cern.ch/tenyears-www/Declaration/Page1.html. Last visited on 9 July 2015.

and hope that no one will read the book.[937] You cannot have it both ways. That is, expectations of retaining control over information published on a global network is contradictory[938] to the nature of the space in which the information was published, where users expect that publicly accessible information is just that – publicly accessible – because the nature of the space is open. No one expects to be obligated to contact a website administrator or owner of a public website ahead of time to secure authorization, and making the information publicly accessible relieves the owner of having to grant individualized access authorization to perhaps thousands or millions of users to the exact same information on a case-by-case basis. The owners relinquish control in return for more efficient, easier access to the information they want to disseminate. For example, arguably much fewer people would use Amazon's services if Amazon tried to retain control of price information by requiring users, every time they were looking to buy a book, to write an email to Amazon to inquire about the price of a book and then await a reply from an Amazon representative that granted them special access to the price information. In this case, it makes good business sense to cut such a redundant and unnecessary time and money cost. Rather, social norms dictate that if you do not want to reveal the information to anyone and everyone you do not publish the information on a public website because you are addressing a global audience when doing so. It is common sense. If the information is published on a public website, it is inherently open.[939] The computer security aspect supports the difference in the nature of the space between open and closed spaces. The security perimeter is a logical perimeter within which all controlled and protected resources are kept. Within the perimeter there may be various domains (protected resources) where the innermost domain is the best protected because it consists of the most sensitive resources. The perimeter of each domain is guarded by access controls, authentication, identification, etc. Those resources that are intended for general public access are placed outside the domain (outside the perimeter) and are expected to be and acknowledged as exposed. The publicly accessible resources are placed outside

[937] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 23. Available at http://ssrn.com/abstract=2601707

[938] Tim Berners-Lee, the inventor of the World Wide Web, explained his reason for giving his invention to the world for free instead of retaining proprietary control over it: *"Had the technology been proprietary, and in my total control, it would probably not have taken off. You can't propose that something be a universal space and at the same time keep control of it."* Quote from the World Wide Web Foundation's website (History of the Web) at http://webfoundation.org/about/vision/history-of-the-web/. Last visited 9 July 2015. Although Berners-Lee was speaking about the Web technology as a whole, the contradiction inherent in the idea of retaining full control and offering universal access at the same time arguably applies equally to those computer owners who publish information on the web making the information universally accessible, and yet expect to retain full control of access to and use of the information.

[939] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 22. Available at: http://ssrn.com/abstract=2601707

the perimeter so that the resources inside the perimeter (within the various domains) are not exposed.[940] Thus, public websites are open spaces[941], not only as a result of social norms, but because they are treated as such for security purposes. This view is arguably supported by legislative history because the committee reports point to computer security as the primary prevention. When resources are placed outside the security perimeter the owner has opted to expose the resources and thus opted out of security (at least with respect to confidentiality), and if an owner has opted out of the primary, most effective method of preventing access, the question is whether mere access, absent damage to the resource, should be protected by criminal law, because authorization and access control is only relevant at the perimeter with respect to entering the perimeter; it is not relevant outside it.

As explained above, companies will implement code-based "restrictions", or "speed bumps"[942] as Kerr calls them, that in combination with terms and cease-and-desist letters that legally (albeit not technically) serve to exclude competitors and their bots, and others, for example those whose business is based on supplementing a service provided by the owner of the website; recall for example the case *Southwest v. BoardFirst*, where BoardFirst's business essentially was spawned from Southwest's way of doing business in that Southwest made their customers compete for the coveted priority boarding passes based on a first-come first-serve principle, and BoardFirst served those Southwest customers who were willing to pay a third-party (BoardFirst) to compete for those boarding passes on their behalf.

If the default status of public websites is "open" and access is authorized, the question is whether owners can construct a "legal fiction" that allows them to selectively exclude whomever they want by implementing easily circumvented code "restrictions", by publishing written restrictions (e.g. Terms of Service), and/or directly revoking the authorization that inherently flows from the technically enabled public accessibility. That is, can website owners transform what is and appears open, to being "closed" by just saying so or by implementing essentially symbolic barriers, not because the barriers are effective, but because their presence, no matter how ineffective, can form the needed thrust of an argument of unauthorized access that terms of service and the likes might

---

[940] Charles P. Pfleeger: Computer Security, AccessScience. McGraw-Hill Education, 2014. Web. 12 July 2015. Section on Security Perimeter.

[941] See along those lines *Pulte Homes v. LIUNA*, 648 F.3d 295, 304 (6th Cir. 2011) ("Rather, like an unprotected website, Pulte's phone and e-mail systems "[were] open to the public so [LIUNA] was authorized to use [them]."")

[942] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 27. Available at: http://ssrn.com/abstract=2601707

not be able to support by themselves. Kerr argues that easily circumvented code "restrictions" such as IP blocking, cookies, CAPTCHA, user agent detection, etc. and terms of service and the likes should not render the access unauthorized.[943] The argument is inherently based on code in the sense that the foundation is the openness of the web, but coupled with the sensibility of questioning whether even symbolic, multi-purpose or easily circumvented code restrictions are perceived as actual, meaningful access restrictions that turns otherwise authorized access into criminal unauthorized access. I agree that the inherent openness of the web should make symbolic attempts to filter out certain people from visiting otherwise entirely public websites irrelevant in the legal sense. However, I am not sure that argument is going to convince judges that a fairly clear notice not to access a website, even a public one, does not override the open norm of the web. Supermarkets can ban a person, libraries can likely ban a person as well from entering. If you have been specifically told not to enter, will a social norm of openness negate the specific ban directed at you? Whereas people cannot disconnect their property from the physical world, people can disconnect servers from the web as a virtual space. Accessibility in virtual space is a choice that requires positive action by the owner.

IP blocking, cookies, user agent detection, CAPTCHA, hard-to-guess URLs and other measures can frustrate access but will not restrict it.

11.5.3.2 IP blocking

For example IP blocking could be aimed at specific people or could be aimed at a range of IP addresses. Most people get assigned dynamic IP addresses that change every so often and thus an IP address would only be effective and noticeable by those who have static IP addresses. But if a new static IP address is requested to a customer upon his request, the IP block – the code restriction – does not exist anymore. A person cannot be forced to retain a specific static IP address (with the associated added costs related to obtaining and maintaining a static IP address), so that a website owner's IP block remains in "effect". Not only would that place an odd obligation on a person, but

[943] See Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), pp. 22-29. Available at: http://ssrn.com/abstract=2601707

could obligate the ISP to reserve that IP address for that customer despite the depletion of IPv4 addresses that necessitates dynamically assigning IP addresses.[944]

11.5.3.3 User-agent string

A user agent is essentially the program through which the user contacts a webserver. It could be a browser, iTunes, or any other program that retrieves resources using HTTP. The user-agent string is sent to the webserver and identifies the software your device is running. The version of the website you are requesting may differ depending on which browser you are using, because of compatibility issues. For example mobile devices will get served a mobile version of the website (if one exists).

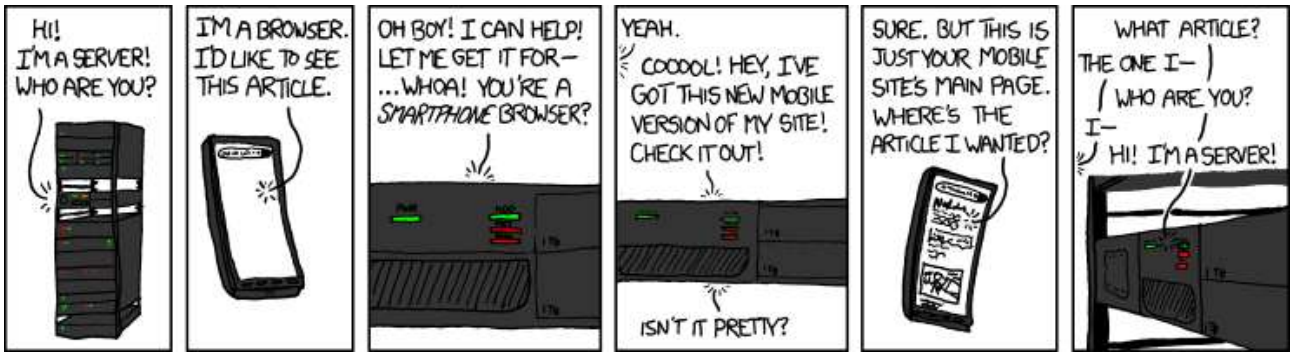


Figure 2 "Server Attention Span". Available at https://xkcd.com/869/.

Here is an example of how to restrict access depending on arbitrary environmental attributes on an Apache webserver as provided in the Apache webserver documentation:

```
SetEnvIf User-Agent BadBot GoAway=1
Order allow,deny
Allow from all
Deny from env=GoAway
```

Warning: Access control by `User-Agent` is an unreliable technique, since the `User-Agent` header can be set to anything at all, at the whim of the end user.

In the above example, the environment variable `GoAway` is set to `1` if the `User-Agent` matches the string `BadBot`. Then we deny access for any request when this variable is set. This blocks that particular user agent from the site.[945]

---

[944] All IPv4 addresses have been or are nearly exhausted everywhere except in the African region. Addresses in the US are expected to be depleted on or around 13 July 2015. See data at http://www.potaroo.net/tools/ipv4/. Last visited on 10 July 2015.

[945] This paragraph and two paragraphs above are taken directly from the documentation/manual for an Apache HTTP server version 2.2, section on "Access control by environmental variable". Available at

As noted in the Apache documentation, access control by user-agent is unreliable, because browser settings are entirely within the control of the user. Switching user agents is commonplace and is done for a variety of reasons, including research, privacy, and improving compatibility. Furthermore, and perhaps importantly, the user-agent string is optional.[946]

A webserver can be configured to restrict access by certain user agents but allow access for others, such as was the case in *US v. Auernheimer*. AT & T had configured the server to be open to iPads, but closed to other devices. Thus, in order to access the website, Auernheimer and Spitler had configured their browser's user-agent string to reflect what AT & T's server allowed, namely, an iPad. As discussed above, almost all of the major browsers "pretend" to be something they are not. Moreover, the user is free to insert custom strings in the user-agent field and can easily do so.[947] If a website is only compatible with an older version of Internet Explorer, is it wrong to change the user-agent to reflect that older version when the browser requests the website? Or should the compatibility problem be understood as an access control aimed at newer versions of Internet Explorer?

Browser fingerprinting has also become a privacy concern, because the user-agent string can uniquely identify users based on their browser's configuration, and thus can be used to track the user. The user-agent string has also been used for the purposes of price discrimination. Because those using the Safari browser on a Mac computer (which is considered a luxury product) are willing to spend more money to obtain a luxury product, they might also be willing to pay more for e.g. hotel stays or trips, or if you are using a mobile device you might get better deals. But is it a crime to change the user agent to check for better deals or to investigate price discrimination? It is doubtful that if price discrimination is based on user agents that a website owner would want that to become public knowledge, or they may construe your access as unauthorized because you gained access to a price that, based on your actual device, you were not supposed to be offered.[948] Should a

---

https://httpd.apache.org/docs/2.2/howto/access.html. Last visited on 12 July 2015. Apache is the most popular webserver today. See June 2015 webserver survey at http://news.netcraft.com/archives/2015/06/25/june-2015-web-server-survey.html. Last visited on 12 July 2015.

[946] See the amici brief in support of Auernheimer at http://torekeland.com/wp-content/uploads/2013/07/Mozilla-Amicus.pdf, p. 7 et seq. Last visited on 12 July 2015.

[947] The option is available through the developer menu in most major browsers. It is available as an addon for Firefox.

[948] See generally the amici brief in support of Auernheimer at http://torekeland.com/wp-content/uploads/2013/07/Mozilla-Amicus.pdf, p. 11 et seq. Last visited on 12 July 2015. See also article on Wired.com,

website owner's choice of (unreliable) access control force you, with the backing of criminal law, to reveal information about yourself? A similar problem presents itself in terms of cookies, which can also make the user uniquely identifiable, but the deletion of which could potentially incur criminal liability for the user. In any case, it is not against the "intended function" of the browser to change the user agent.

11.5.3.4 Cookies

Cookies can be used to erect a rather flimsy "wall". For example, many online newspapers put a pressure on the user to purchase a subscription after the user has read ten articles for free (perhaps within the course of a month). Some of you may have noticed this "barrier" and others almost never encounter the barrier. The difference lies in your stance towards browser cookies. Browser cookies are tiny bits of data that are sent from a website you visit and stored by your browser.[949] The protocol the web uses is HTTP (Hypertext Transfer Protocol). HTTP is designed to be simple in that a web of information should be accessible to any system regardless of design differences. HTTP, in its simplicity, is stateless,[950] which means that a website will not remember you from page to page on the site unless something makes the session "stateful". Thus, the website sends a cookie containing state information to be stored in the browser. The cookie allows the website to track you as you surf the site, for example, so that it does not forget the contents of your shopping cart as you browse other products, or so that you remain logged into your account as you browse pages on the website. However, you remain in control of the browser and thus the cookies that the website sends to your browser for storage. Those concerned with online privacy and the use of cookies to track their movements e.g. for the purposes of targeted advertising[951], may be familiar with browser features that let you delete cookies manually, let you direct the browser to delete all cookies upon exiting the browser, or for example let you configure your browser to not accept

---

Ashkan Soltani: Protecting Your Privacy Could Make You the Bad Guy (23 July 2013). Available at http://www.wired.com/2013/07/the-catch-22-of-internet-commerce-and-privacy-could-mean-youre-the-bad-guy/. Last visited on 12 July 2015.

[949] See RFC 6265 (proposed standard), section 3. Available at https://tools.ietf.org/html/rfc6265#section-3. Last visited on 10 July 2015.

[950] RFC 2616, Abstract. Available at http://www.rfc-base.org/txt/rfc-2616.txt. Last visited on 10 July 2015.

[951] Persistent cookies (those that have an expiration date set, instead of expiring when exiting the browser) may be sent to the server specified in the cookie whenever a resource from that server is present on a third-party website, e.g. an advertisement, beacon, etc. An example of such a resource is Facebook's ubiquitous "Like" buttons. When loading a website that contains advertisement, images or other resources that are retrieved from a third-party website cookies can be set and/or sent for each of those third-party websites.

cookies at all. The cookie set by a newspaper website when you visit the website, gets sent back to the website when you access it again and thus the cookie can keep track of how many articles you have read, given that the cookie has not expired. Those who clear the cookies in their browser for privacy reasons, or other reasons, may not ever or seldom be faced with the technical "barrier" that the cookie may present.

Cookies can thus interfere with access to public websites e.g. when they are used keep track of the number of free articles read and create an obstacle for some users. The question is whether cookies can justify a deviation from the authorization to access that is inherent with regard to public websites, and whether a user who deletes the cookies in his browser and e.g. continues to read articles on a news website is circumventing a code restriction, such that he triggers the application of unauthorized access statutes.

Kerr argues that cookies are just speedbumps and not barriers. "It's just trying to create enough of a hassle to push some users to buy a subscription to avoid it."[952] But ultimately, as Kerr also recognizes, the browser is controlled by the user, and the user decides whether to allow cookies, delete cookies or keep cookies.[953] As with switching user agents, it is not against the "intended function" of a browser to delete cookies.

What Kerr appears to argue is that a public website's[954] code restrictions that are essentially implemented client-side (i.e. on the user's end) rather than server-side (i.e. on the website owner's end), and for that reason are within the user's control, are not code restrictions the circumvention of which ought to incur liability for the user under unauthorized access statutes.

---

[952] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 25. Available at: http://ssrn.com/abstract=2601707

[953] Recall the user-agent discussion in connection with *US v. Auernheimer*. Kerr also rejects a user's browser's user agent settings as a liability-triggering code restriction, since user agent settings, just like cookies, are completely within the user's control.

[954] Note that e.g. stealing session cookies of an authenticated user or manipulating cookie values and thereby gaining access to someone else's *closed* account mirrors the concept of using someone else's password. That is, the nature of the space of an account that requires authentication differs from that of the *open* publicly accessible website.

11.5.3.5 CAPTCHA challenges

CAPTCHA as an access control is, however, implemented server-side. The purpose of a CAPTCHA challenge is to hinder automatic access to a certain resource by a non-human actor.[955] However, as mentioned before, CAPTCHA also keeps out human actors, such as the visually impaired, dyslexic, etc., although that may not have been the website owner's intent when implementing CAPTCHA. Thus, if CAPTCHA circumvention is unauthorized access, then the CAPTCHA circumvention is criminal regardless of the website owner's subjective reason for implementing CAPTCHA and criminal regardless of the user's motive for circumventing it. For example, in *US v. Lowson*, Ticketmaster's primary concern seemed to be keeping out actors like Lowson who access the site for financial gain. Although Lowson's conduct may have been disruptive and perhaps triggers criminal liability under other provisions or subject to civil liability, his conduct would have been equally undesirable had he hired human actors to respond to the CAPTCHA challenges. A human actor responding to the CAPTCHA challenge would not constitute circumventing a code restriction solely based on the actor being human, and thus, it is clear that the issue is not with access to the site per se or information on the site, but the purpose for buying the tickets, namely, financial gain. The First Circuit noted, in terms of automated access, in *EF v. Zefer*: "Needless to say, Zefer can have been in no doubt that EF would dislike the use of the scraper to construct a database for Explorica to undercut EF's prices; but EF would equally have disliked the compilation of such a database manually without the use of a scraper tool. EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns."[956][957] Although, Lowson was competing with Ticketmaster by buying blocks of tickets from Ticketmaster and selling them in the secondary market, the principle is the same; Ticketmaster would have disliked the conduct whether the access had occurred by way of non-human actors or human actors.

---

[955] See e.g. weakness definition of CAPTCHA guessing on MITRE's Common Weakness Enumeration (CWE) website at https://cwe.mitre.org/data/definitions/804.html. Last visited on 11 July 2015.

[956] *EF v. Zefer*, 318 F.3d 58, 63 (1st Cir. 2003)

[957] Note that in *EF v. Explorica*, Explorica was found to have violated the "exceeds authorized access" prong, not the "without authorization" prong. Thus, even though Explorica had authorization to access the website, the court found that they had exceeded their authorization by using a scraper to access. That is, the "means of access" meant that an otherwise authorized access was turned unauthorized, because the "context of the access" (the existence of a confidentiality agreement) enabled the "means of access".

11.5.3.6 URL manipulation ("URL hacking")

URL hacking, or URL manipulation, refers to both criminal and innocuous user behavior, because all it entails is the manipulation of the URL. URL hacking sometimes may refer to e.g. SQL injection[958], that is, the injection of malicious code into the URL string in order to interact directly with the SQL database.

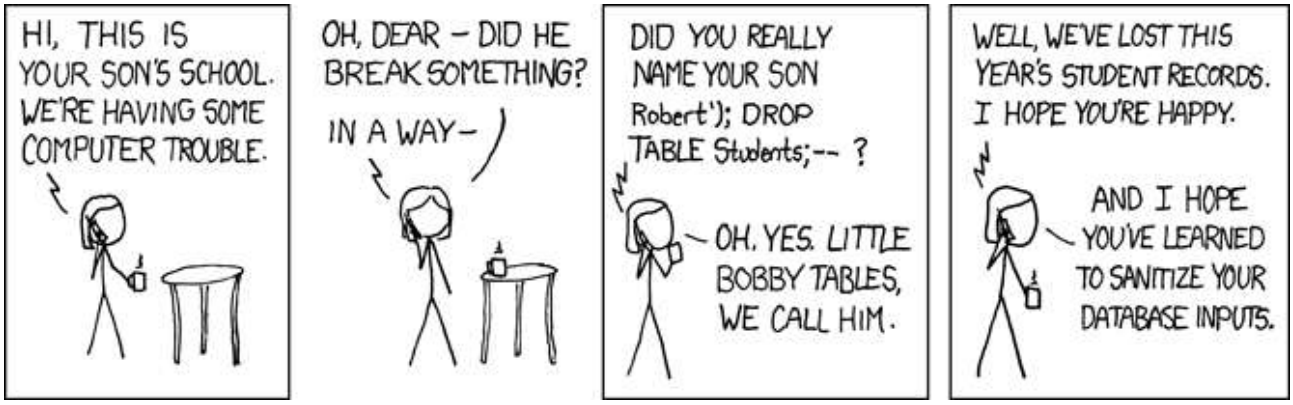


Figure 3 "Exploits of a mom"; available at https://xkcd.com/327/

The above comic strip from the website xkcd.com, is an example of SQL injection. By entering the boy's name `Robert'); DROP TABLE Students;--` (SQL code) into the system, a database command was inadvertently allowed to be passed to the database from a field that should only accept text and not e.g. special symbols; that is, the person entering text into a field was inappropriately allowed to execute commands through a field that should only accept text. This is what the mom means when she says that the school failed to sanitize their database inputs; special symbols should not be allowed to be passed that enable execution of arbitrary code. There are few if any circumstances where it would be acceptable for a user to inject SQL code into queries since doing so can potentially allow the user to take over the server, delete tables in the database, access confidential information inside the security perimeter by bypassing access controls, etc. That is, it is

[958] SQL code injections into the URL. There are three types of SQL injection methods, (1) error based, which is the simplest – one gets the database to reveal information about itself and eventually dump the username and password columns into the browser window; the error windows reveal the information gradually as you probe the server through commands; (2) union based – based on the SQL union command; (3) blind based, which is the hardest method that usually would require a few days' work. Websites with weak security can be revealed simply by googleing "admin/login.asp?id=", follow the link to the login page and type in admin as username (there is almost always a username called admin) and in the password type some SQL statement that the database will always recognize as true, such as "'1 OR '1'='1'", which means you are asking the server whether 1 = 1, which of course it will agree with you is correct and therefore grant you access, unless adequate precautions have been taken by the administrator and all database commands inputs have been filtered out from website forms. Sometimes the web administrator has only bothered to sanitize the password input for the 1 = 1 command, as this is first thing hackers will try. This means that a hacker can just ask it whether 2 = 2, and get past the filter.

not the intended function of the URL address bar and the user input fields on websites to be used as a means of bypassing password or other security mechanism that protect the database inside the perimeter, or to cause damage to the server or elevate the user's privileges on the server.[959] SQL injection is akin to Morris' exploitation of vulnerabilities in the SEND MAIL program and the finger daemon; outside the social norms of means of access. But just because SQL injection through the URL address bar (or elsewhere) is malicious does not mean that any manipulation of the URL is criminal.

URL hacking is also sometimes used to refer to simply adding to, changing or in some other way editing the URL string to browse a website, retrieve certain webpage content or resources, view a particular news article, change the language of a page, returning to the home page, and so on, instead of using the hyperlinks that may or may not be provided on the website.

Criminal URL hacking could perhaps be defined as that involving the injection of code into the URL query strings in a way that departs from the intended function[960] of URLs as resource locators rather than general command line interfaces.[961]

Alternatively, a comparison to trade secret law principles perhaps casts some light on the viability of a concept of "secret URLs"; e.g. principles of reverse engineering[962]. Information is not a trade secret if it is publicly known, independently discovered (e.g. reverse engineered) or guessed.[963] For example, where the components in the URL might follow open standards, such as was the case in *US v. Auernheimer* it is hard to argue that the component is secret or that the URL as a whole is secret because it was discoverable, guessable or capable of being reverse engineered. Furthermore, comparing it to a password is futile because the open standard necessarily implies the absence of secrecy. The purpose of bringing up trade secret law principles is not to import trade secret law principles into hacking statutes, because trade secret laws and hacking statutes protect different things (whereas trade secret law covers improper obtaining of information, unauthorized disclosure and unauthorized use of trade secrets, the CFAA covers unauthorized access to computers and information one is not authorized to access, but not disclosure or use of information). But the

[959] The same concluded in Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 28. Available at: http://ssrn.com/abstract=2601707

[960] Akin to the "intended function" test employed by the Second Circuit in *US v. Morris*.

[961] The intended function should never be derived from how the plaintiff intended the URL to function, because regardless of the plaintiff's influence on what components figure into the URL on the plaintiff's website, the plaintiff cannot redefine documented standards to suit his specific desire for legal consequences. Such ad hoc subjective redefinitions of the functions of URLs are clearly undesirable. The owner's sphere of control in terms of a website should not be extended to definitions of technical schemes and standards that concern the function of the Web and the Internet in general.

[962] See more about reverse engineering in Danish law in Henrik Udsen: De informationsretlige grundsætninger (2009), p. 299

[963] See e.g. Restatement (Third) of Unfair Competition § 43 (1995)("[…] Independent discovery and analysis of publicly available products or information are not improper means of acquisition.")

trade secret law analogy is useful in terms of showing that if a URL is guessed, a website's structure deduced, etc. it cannot be a secret. As soon as the URL is discovered, it is no longer secret and access is authorized.

There is a difference in norms between guessing a URL and injecting malicious code into the URL and thus sending malicious code to a database.

11.5.3.7 Summary

IP blocking, restricting certain user-agents, cookies, CAPTCHA challenges and hard-to-guess (or generally guessable, deducible) URLs share a characteristic; in the context of public websites they are used to create fictional perimeters where the resources are already exposed to the general public. They are an illusion of security against access to the resource whilst they in reality provide none and the resource is as exposed as before.

Where bots are purposely designed to affect the availability of the exposed resource, § 1030(a)(5)(A) would still be applicable, since this subsection does not require that the access was unauthorized, but rather that the damage was caused intentionally and without authorization. However, subsections (a)(5)(B) and (C) do require that the access was unauthorized in order to cover damage that was caused recklessly and simply causing damage (without any scienter requirement as to the damage). Thus, if authorization to *access* to the exposed resource outside the perimeter (in the open space) is irrelevant, the CFAA would ostensibly fail to cover e.g. badly coded bots the use of which might recklessly cause damage to (affect the availability of) exposed resources such as public websites.

Kerr's, and arguably, the Second Circuit's (in *Morris*) social norms-based approach (particularly nature of the space) is ostensibly a reflection of computer security in the sense that the concept of perimeters, the protected resources being domains that the perimeter encloses and the exposed resources being those outside the perimeter, i.e. out in the open. The means of access become relevant only when the means damage the exposed resources or enable entry into the perimeter (access to protected resources). The context of the access is also only relevant with respect to entering the perimeter. Where the means of access are not at odds with the program's or code's intended function (the social norms attached to means of access), the social norms governing the context of the access may still render the access unauthorized; for example in situations where access was gained by password-guessing, using known passwords, etc. where the authorization of the account owner is absent. Entering a password, regardless of delegation of authorization to

access using that password, does not violate social norms with regard to means of access, but it is captured by the norms governing the context of access.

Switching IP addresses and user agents, deleting cookies, and deducing URL addresses from an observable context is so commonplace and trivial that considering those switches, the deletion or deduction as a trigger for criminal liability under hacking statutes appears to be a rather serious case of overcriminalization, when said conduct only leads to continued access and obtaining of an already exposed resource (i.e. a resource placed in an open, publicly accessible, space).

11.6 A possible Danish interpretation: Revisiting the suggested "reasonable expectations" test in the Danish 1985 Committee Report

The Danish committee, which proposed the hacking provision (§ 263(2)) in the criminal code, seems to have presumed that trespass norms would apply also with respect to analyzing when access under § 263(2) is with right. There is no further explanation of this in the committee report, but it is clearly a reference to social norms related to § 263(1) (privacy of communications, chattels, etc.) and § 264, both of which (including their subsections) concerned themselves with physical space.[964] To revisit what the Committee stated in its 1985 report:

"As with the other privacy violations, violations of the suggested provision will comprise a person gaining access to something, which with respect to them can **reasonably be expected** to be a restricted area, that is, inaccessible."[965] [966]

[964] It appears there has not been much written about the trespass provision in the Danish criminal code (§ 264) and the norms that determine when entry is unauthorized. At least there is not, to the author's knowledge, any Danish literature that explores a comprehensive analytical framework for analyzing authorization in trespass cases. There is a brief discussion in a 1971 Committee report on privacy violations that is useful. The discussion on trespass (§ 264) in Committee report 1971 no. 601, p. 34, does not explicitly use terms like "nature of the space", but it does compare various types of locales and how standards of trespass differ between those locales; e.g. differences between residential houses, openly accessible hallways or stairwas in apartment buildings, building sites, etc. Similarly, the report discusses means of entry briefly and how that may affect whether entry was authorized. Context of entry is also briefly implicated in the discussion on residential houses. Thus, it may arguably be derived from the report that the Committee's thoughts on trespass analysis include (1) the nature of the space, (2) the means of access, and (3) the context of access, showing that these concepts of the traditional trespass doctrine are not common law or US law idiosyncrasies.

[965] Committee report 1985 no. 1032, 25

[966] Emphasis added

Given the language of this quote from the Committee report, the relevant reasonable expectations are those of a person accessing an area (in the objective sense), not the reasonable expectations of the owner of the space.

As demonstrated via the prior analysis of *EF v. Explorica* and *EF v. Zefer* in the above section on "without right" in the Danish hacking provision, a reasonable expectations test is appropriate only where a social norm exists; i.e. a common understanding. The test, as carried out by the district court in *Explorica*, arguably, relies heavily on the fact that the court knew that EF disliked Explorica's use of the website and was seeking to prevent Explorica's use of the information on EF's public website. However, the circumstances that the court relied on to "deduce" lack of authorization was rooted in EF's subjective interpretation of the functioning and meaning of hyperlinks, dropdown menus, the copyright symbol, etc. That is, the court appears to have relied on what EF intended those things to mean, regardless of how society at large would interpret their function and meaning. Probably, the court used EF's subjective expectations as "indicators" that the access was unauthorized, because it was ostensibly clear to Explorica that EF would object to the purpose of Explorica's access to the website (i.e. Explorica's later use of the information to compete more efficiently with EF). Applying a reasonable expectations test rooted in the subjective expectations of the owner would render the application of hacking statues arbitrary and unforeseeable.

Since it is a question of whether a user (presumably, objectively, a person in his position) could reasonably expect the access to be unauthorized, there is a tie to social norms associated with the nature of the space, the means of access and the context of the access. Recall that the Danish hacking provision is a subsection of a privacy provision; the open nature of the web should make an owner's objection to access to public websites irrelevant under the hacking provision, even if the user suspects that the owner, if asked, would not approve of the access or would not approve of access for certain purposes.

However, as follows from the social norms governing the means of access, not every interaction with a public website is necessarily authorized just because it is open space. However, is it not the access to the website itself that is objectionable; rather, it is the access that could be gained through vulnerabilities on the website, such as would be the case with SQL injections, or by guessing passwords etc.; i.e. moving into a closed space.

Furthermore, in the physical realm, the code-based approach fails when code does not restrict access to a computer, but where the access is clearly contrary to social norms, a social norms approach would remedy the short-comings of the code-based approach. A pure code-based approach, furthermore, suffers from the flaw that code can be interpreted in many different ways. For example, under the code-based approach it was brought up that code restrictions can, and has been, interpreted quite widely; the widest perhaps being the district court in *Explorica* interpreting hyperlinks and dropdown menus as a restriction on any other method of browsing. The code-based approach is arbitrary, because it does not leave room for distinguishing between what code we perceive as actual restrictions and code that we do not perceive as actual restrictions.

Criminal liability based solely on the breach of contract (terms of service, terms of use, etc.) should be rejected. A contract-based approach carries with it highly suspect foreseeability issues and issues related to arbitrary enforcement. Furthermore, under Danish law, contractual breach does not automatically discharge the contract[967]; instead remedies become available to the other party, one of which may be termination of the contract, but generally only if the breach is a fundamental one. Thus, even if there has been a breach of contract, not any and every breach necessarily triggers termination of the contract as a remedy.[968]

As it stands, Danish law arguably supports Kerr's view that terms of use and terms of service merely state the owner's right to terminate access to a closed account (by blocking the account or deleting the account). It does not under any circumstances serve as an automatic trigger of criminal liability, since not even civil contractual breaches could normally lead to the automatic discharge of the contract and trigger civil liability without further action on part of the owner.

The social norms approach is, in part, inherently built upon code, because code shapes what we see and what we can do online (and computers, generally). It is code that partially informs us of the intended function of a program, which is then further supplemented by social norms, i.e. what the intended function is generally understood to be. But make no mistake, the code does draw the initial boundaries of what is and is not possible.

[967] See e.g. Mads Bryde Andersen and Joseph Lookofsky: Lærebog i obligationsret I – Ydelsen Beføjelser (2009), p. 209

[968] See e.g. Mads Bryde Andersen and Joseph Lookofsky: Lærebog i obligationsret I – Ydelsen Beføjelser (2009), p. 210

A careful and informed application of an objective social norms approach corrects the arbitrariness inherent in both the code-based and contract-based approaches, and will likely, if applied objectively, put the user on sufficient notice of what is criminal and what is not. It would furthermore bar owners from implementing arbitrary and/or questionable code barriers that do not actually restrict access, although they might slow it. Such code barriers are often inextricably linked to terms of use or terms of service (which on their own are rarely enforceable in absence of a code barrier, regardless of its efficacy as such), which in themselves might be arbitrary and, as a policy matter, undesirable to enforce as a criminal offense. Contractual terms and trivial code restrictions would make criminals out of a vast number of the general public, for example those who use VPN servers to access entertainment services in other regions and those who delete their browser cookies for privacy reasons but continue to access newspaper websites who use cookies as "pay walls". Surely, more is needed to convict and punish under a hacking provision.

As to the social norms related to computers, it cannot be stressed enough that it is exceedingly important for the judge, the prosecution and the defense are well informed about the technical aspect of cases. Otherwise, what are common practices (norms) in computer circles could be misunderstood as being nefarious solely because the actors in the legal system do not understand the technology. Thus, the norms ought to be based on what is commonplace conduct to those who work in the IT industry, rather than what would be acceptable from the viewpoint of the average-Joe who cannot relate to or does not understand commonplace practices that may sound nefarious or odd; it ought not be based on fear or suspicion of the unknown, but on knowledge and experience. Contrary to the prosecution's claim in its opening statement[969] in the biggest and most complicated Danish hacking case to-date, understanding the technology is not irrelevant or inconsequential to the adjudication of the case, because anything that is unknown and complex may be approached with inapposite and unnecessary suspicion or apprehension. A juror's or judge's life experience cannot substitute or negate the need for knowledge about the technology that enables the juror or judge to understand the evidence and the norms in IT contexts.

The Danish hacking provision in the criminal code's § 263(2), although its scope of its literal language is much broader than its US federal counterpart, has limited application with respect to

[969] See e.g. Version2's coverage of the district court trial. The prosecution's claims were noted by reporters covering the trial, http://www.version2.dk/artikel/anklager-i-hackersag-man-kan-ikke-foele-sig-sikker-paa-sin-straffeattest-68452. Last visited on 14 July 2015.

publicly accessible resources. Given that the information on publicly accessible websites/servers is made technically accessible to anyone connected to the Internet, the owner's consent or subjective intentions related to any access to those publicly accessible websites is irrelevant to the evaluation of whether the access was without right – at least under Danish law and under the Convention.

Neither the Danish hacking provision's language nor the language of the Convention's article 2 excludes publicly accessible resources from their scopes, but it is patently clear from the legislative history of the Danish § 263 and Explanatory Report's explanation of the scope of the Convention's article 2 that access to publicly accessible resources such as websites must to fall outside the scope of the criminalization. The Danish provision already suffers from linguistic deficiencies that arguably bar its literal application, because the Danish provision does not require that the information resides on a computer; it can reside on paper for later use on a computer, which, if the provision were applied literally, would criminalize unauthorized access to information on paper.[970]

In the Committee Report 1971 no. 601 on amendments to the chapter on privacy violations, the Committee explained in connection with privacy of communications (letters and such), which is another subsection under § 263[971], that reading a letter that the owner has left open in an area where he could expect others to travel through, the owner renounces any right to protection under the provision. Therefore, even if no distinction is made between private and public websites, information or servers in connection with subsection 2, it would be counterintuitive to protect a public website (where more people, possibly in the thousands or more, are likely to "travel") and not a private letter left out in the open where maybe only a handful of people travel – especially considering the provisions being placed in a chapter on privacy violations. So on this basis it can be concluded that, in Danish law, presumably there is a "scale" of sorts when it comes to imposing liability for accessing information that ranges from "public" to "private/non-public". It would be odd to argue the "letter left out in the open" case as a case of the letter owner's consent for by-passers to access its information, rather than simply seeing it as the owner losing the right to protection under the law in terms of that letter.

[970] Several US courts applying § 1030 have stated that there is nothing ambiguous about the statutory text that requires examining legislative history. A US court could say the same if they were to interpret the Danish criminal code's § 263(2); namely, that the legislature could have passed a provision that required the information to reside on a computer, but neglected to do so.
[971] Danish criminal code § 263(1)(1)

Professor Henrik Udsen argues in his book *De informationsretlige grundsætninger*[972] ("Doctrines of Information Law"), in the data privacy law context, that just because it is obvious that the website is only intended to be accessed by friends and family for example, and only those few people are familiar with the URL of the website does not negate that the possibility of others visiting the website, that being an acknowledged and accepted fact; regardless of whether others actually do visit the website or not. Udsen therefore concludes that the main rule must be that information *made accessible* from a website absent code-based restrictions with the consent of the "registered person" is published within the context of the Danish Data Privacy Act § 7 (2)(3).[973] The "registered person's" consent would only be relevant in terms of whether the information was *published with right* – but the consent is not relevant when determining whether the information was or was not in fact actually *published* (made accessible) from a legal perspective. Udsen further argues that as opposed to newspapers, TV, and radio, where one can legitimately presume that the information has *in fact* been published to a large number of people, the same presumption cannot be transferred to the Internet where websites are technically accessible to any person in the world with an Internet connection, even though most web sites are rarely visited by a large number of people. That is, the *possibility* of widespread publication is in itself enough – the website need not be known or accessed by anyone for the information to be considered published within the context of data privacy law.[974] This resonates well with the fact that within the context of the Internet, users request the web pages of interest from the web server, unlike TV, newspapers and radio where the user generally receives the information unprompted (apart from turning on the television and perhaps being contingent on being a subscriber for a signal to be delivered) and presented in a form and with such content as deemed fitting by the provider. The Internet users "pull" the information from the service providers rather than the service providers "push" it to the users. This should, however, not change the fact that the person receiving the information from a publicly accessible source is not responsible for it being publicly accessible in the first place.

Two separate instances of the so-called "URL hacking" were carried out by Reuters journalists on websites belonging to the Danish company Topdanmark[975] and the Swedish company Intentia.[976] Both cases involved making minor changes

[972] Henrik Udsen: De informationsretlige grundsætninger: Studier i informationsretten (2009)
[973] Henrik Udsen: De informationsretlige grundsætninger: Studier i informationsretten (2009), p. 304
[974] Henrik Udsen: De informationsretlige grundsætninger: Studier i informationsretten (2009), pp. 303-304
[975] See coverage of the Danish incident on version2.dk. Available at http://www.version2.dk/artikel/finanstilsynet-politianmelder-topdanmark-efter-url-hacking-17251. Last visited on 13 September 2015.
[976] See coverage of Swedish incident on idg.se. Available at http://computersweden.idg.se/2.2683/1.31518/oklart-klockslag-raddade-reuters. Last visited on 13 September 2015.

to the URL, e.g. that logically the year after 2004 is 2005, so the 4 would be changed to 5 in the URL. On October 24th 2002 the Swedish software company Intentia planned an official release of the company's report on its third quarter results. The release was planned for 'around' two o'clock in the afternoon. Nevertheless, a couple of hours before the scheduled release, a journalist from Reuters had found the report by changing a few symbols in the URL address for the report from the previous quarter. The report had been placed, without access restrictions, on Intentia's web server. Intentia claimed that it was "hacked" by the Reuters journalist as no hyperlink had been provided to the report by Intentia. For that reason the journalist had, in Intentia's opinion, committed the crime of "dataintrång", which essentially translates to unauthorized access. The Swedish prosecutor Håkan Roswall decided against prosecution of the Reuters journalist for several reasons. First, Intentia had announced a release of the report "around" two o'clock in the afternoon. Since the time of release had not been precisely specified, the prosecutor claimed that this factor alone would be extremely problematic for establishing mens rea, as the reporter could not reasonably have known whether the access was unauthorized or not. Roswall did state that the situation may have been different had Intentia specifically announced the release of the report at precisely two o'clock. Thus, a journalist accessing the report before the specified time would have the mens rea required, since the journalist would then have reason to suspect he or she was accessing the file illegally. Secondly, as stated by the prosecutor, the file was placed on an open web server granting public access. Thus, the information cannot be considered private without any further indications of it being private. Simply neglecting to provide an official link to the individual web pages did not change that default public status of the information, which followed its placement on an open web server. Therefore, the actions of the Reuters journalist could not reasonably be considered to fall within the scope of the actus reus of the crime, namely "unauthorized access", since access by any and all members of the public was without any restrictions.

In the Danish Topdanmark case, which is factually almost identical to the Intentia incident, the report's publication time given on the website was specific, a police report was filed, yet no charges were filed against the journalist nor did any prosecution official comment on the case. The company only seemed to claim hacking as a defense against the criminal charges it faced due to the inappropriate distribution of insider information that took place because of the absence of proper security measures. The journalist had simply changed the "year" value in the URL.

It begs the question whether URLs can be claimed to be "secret" and constitute a password of some kind, and therefore be perceived as a "technical barrier" of sorts. Technically, speaking it is impossible to distinguish between a "secret" URL and a password[977]; therefore, one can only reach one rather inconvenient solution that if passwords are technical barriers then "secret" URLs must also be technical barriers. However, there are fundamental differences between how people generally perceive URLs and how they perceive passwords.

In another case involving the retail store Harald Nyborg and a website security incident, the customer reported having been threatened by the company. The customer had reported the incident to an online magazine after allegedly having urged Harald Nyborg several times to fix the problem. According to the account given by the customer to the

[977] Thanks to associate professor René Rydhof Hansen, ph.d. (IT security), for helpful discussions on this topic.

newspaper, he had received a letter from Harald Nyborg threatening to file suit if the server or software was in any way damaged as a consequence of the customer's disclosure of the leak to the online magazine.[978]

Although it is still uncertain whether Danish courts would consider URL hacking to be unauthorized access, an application of the social norms approach, discussed above, would result in URL hacking being authorized access due to the nature of the space being open and the means of access do not conflict with the intended function of URL addresses. This conclusion is furthermore supported by the fact that neither Topdanmark nor Intentia took precautions to that would change the nature of the space to closed by requiring special permission – thus, clearly indicating that the reports were not yet accessible to other users than those specifically authorized.

A social norms approach, such as the one Kerr has derived from *Morris*, does not appear to be at odds with the Danish hacking provision or its legislative history. In fact it seems to fit quite well given the references to reasonable expectations depending on the nature of the space. The means of access and the context seem to be rather natural considerations, as well – regardless of the legal system.

[978] Reported on the website of the magazine Computer World on July 11th 2002 (in Danish); Jens Bertelsen, 'Harald Nyborg truer kunde med krav om erstatning' (2002) http://www.computerworld.dk/art/15316/harald-nyborg-truer-kunde-med-krav-om-erstatning accessed June 23rd 2014

11.7 Summary

The above analysis of the code-based approach shows that although the approach successfully narrows the scope of hacking statutes (under the assumption that "authorization" puts the primary limitation on the scope) by asking whether the code allowed the user's conduct, the approach is too narrow in some respects and too broad in other respects. It appears to be overly accepting of even arbitrary ideas of code restrictions, and, particularly, it provides peculiar protection against the obtaining of information from public websites. The code-based approach is too narrow in the sense that it will fail to protect against clearly unauthorized access to computers which are not protected by code against those who have physical access to the computer (rather than remote access). The approach thus both over- and undercriminalizes. It could be argued that where arbitrary restrictions to access public websites are enforced, those restrictions may often be a translation into code of contractual terms, the breach of which is often not enforceable under hacking statutes (and the criminal enforcement of which would be unforeseeable).

The contract-based approach essentially allows computer owners to define the scope of criminal conduct. Contractual restrictions can be entirely arbitrary in nature, ranging anywhere from violating the "spirit of the statement" (Facebook's terms of service) to more specific infractions such as lying about personal information such as name, age and gender, or failing to keep said personal information up-to-date.[979] In other words, there are no limits to the scope of hacking statutes if the contract-based approach is followed. Keeping in mind that, as a rule, breaches of contract do not automatically trigger the discharge of the contract, but provide the aggrieved party with certain remedies, one of which may be the avoiding of the contract if the breach is a fundamental one. Even so, the aggrieved party must notify the party in breach of the contract that he intends to avoid the contract; it does not happen automatically. Thus, it would be particularly odd to allow a breach of contract, even a non-fundamental one, to trigger criminal liability where the authorization to access could not automatically be revoked civilly. The contract-based approach, due to its arbitrary nature and the discord with civil law remedies, leaves the definition of criminal conduct with computer owners and its criminal enforcement at the whim of prosecutors enabling them to pursue their personal agendas. In other words, the contract-based approach is sure to trigger the application of void-for-vagueness doctrines, such as that under article 7 ECHR, because the

[979] See e.g. Facebook's "Statement of Rights and Responsibilities", clause 4(7). Available at https://www.facebook.com/legal/terms. Last visited on 2 September 2015.

approach leaves the scope highly unforeseeable and introduces a serious risk of arbitrary enforcement.

The social norms-approach is a far more appealing approach than a pure code-based approach (since the approach arbitrarily provides protection) and the contract-based approach (unforeseeable and arbitrary). This approach entails the analysis of three factors; 1) the nature of the space, 2) the means of entry/access, and 3) the context of entry/access. For example, if the space is open, such as a public website, there is presumably no criminal protection against access to the public-facing parts of the website. The context of the entry should not be understood as an inquiry into the purpose of entry of a person who is authorized to access, but does so for objectionable reasons. Rather, the context can clarify the meaning of authorization where there person would generally be unauthorized to access, but does so for a socially recognized purpose, such as the mailman entering the property to deliver the mail, or where a person who is not authorized but does not gain access through objectionable means, e.g. a person guessing a password to access a closed space (without the means of access being suspect as such, i.e. against the intended function) under circumstances where no delegation of authority from the owner has taken place. The social norms-approach is not free from consideration of code. In fact, code inherently defines the nature of the (virtual) space, because the code provides the framework for the space (whether it is open or closed) and thus naturally influences the social norms that will later attach themselves to that particular space. Furthermore, code provides the framework for the means of access. However, code free from interpretation as a legal basis for a criminal conviction will produce absurd and arbitrary results and hence results that are irreconcilable with social norms; including both cases where the conduct was clearly unauthorized even though the code did not prevent the access, and cases where code (perhaps contract-inspired) arbitrarily triggers criminal protection of use of and access to publicly accessible information. The social norms approach can be said to correct and amend the code-based approach in that the social norms approach does not disregard code but injects some common sense and foreseeability into the analysis of authorization in a virtual environment as well as reducing, to some extent, the risk of arbitrary enforcement compared to the risks associated with a pure code-based approach and the contract-based approach. However, a social norms approach, if construed too liberally, can drastically increase the risk of arbitrary enforcement and reduce foreseeability if social norms are construed to mean e.g. “courteous” conduct or construed as prohibiting “annoying” conduct. Therefore, it is important to remain focused on the three prongs related to the *access*; not on the purpose of the access where access is generally authorized or on the subsequent use of

information obtained through the otherwise authorized access etc. Thus, ultimately, what matters is whether society recognizes the computer owner's expectations of protection against trespass; hence, barring indiscriminate, surprising and/or arbitrary criminal enforcement of ambiguous, broad statutory language that may be at odds with the constitutional and/or human rights related to due process, clarity of criminal law provision, etc. The social norms in the computer context need time to develop; norms related to traditional trespass did not develop overnight. The space, particularly the virtual space, associated with computers and networks is different from physical space. Simply indiscriminately transferring traditional trespass rules into the computer context, by relying on (often inappropriate) analogies, ignores the differences between the spaces.

Finally, as importantly noted by numerous US federal courts, Marco Gercke (in the context of the Convention on Cybercrime and several domestic legal systems), Orin Kerr, and others, it is imperative to separate the *access* from *subsequent conduct* (typically, this is accomplished by inquiring into the purpose of the access) that is either illegal and/or a breach of contract. This problem is ostensibly only relevant where the defendant had implicit or explicit authorization to access. Allowing other legal rules concerning subsequent acts to negate authorization opens up the scope of hacking statutes giving them enormous reach. For example, access to information for the purpose of violating any law would automatically also trigger liability under the hacking statute. This would make breaches of data protection law, copyright law, trade secret laws and other laws regulating use of information, or even generally prohibiting the subsequent conduct, such as processing personal data in excess of what is necessary and online piracy, fraud etc. These illegal acts are not related to *access* to information, but the subsequent *use* of information. Rather the access, in combination with other facts, may be indicative of an attempted crime that directly prohibits a specific use of information, such as disclosure of trade secrets. This distinction between *use* and *access* is no less important in the context of outsiders than it is in the context of insiders.

12 AUTHORIZATION - INSIDERS

The threat that insiders pose to companies, governments and other organizations has frequently been called one of the most serious security issues.[980] The clear distinction there once was between insiders and outsiders has become increasingly fluid and vague due to the use of the internet and the general pervasiveness of computing.[981] One common denominator seems to recur in papers on insiders and insider threats is that the issue centers around the "unique security threats arising from [the insider's] privileged status."[982] Who is an insider and how that privileged status is acquired (legitimately or not) is disputed.

The CFAA's (a)(2)(C) and several other provisions in the CFAA distinguish between "without authorization" and "exceeding authorized access". Only the latter is defined in the CFAA, but the definition is still hinged upon "authorization" which remains undefined by the legislature.

In Denmark, the hacking statute (criminal code § 263 (2)) prohibits access without right to information and programs intended for use on an information system. Decreasing the level of abstraction from computers to information and programs arguably makes a specific "exceeding authorized access" term unnecessary, since the statute reaches beyond the initial authorized access to the computer itself in that it targets access on a lower level of abstraction (the information and programs rather than the computer as a whole). However, as will be evident after the analysis in this chapter, regulating insiders and outsiders with the same language, that is, without distinguishing between the two in the statutory language, is troublesome.

The crux of the matter though is that distinguishing between insiders and outsiders in statutory language is very difficult to do clearly. But the consequences of not distinguishing between the two in statutory language means that the courts' construction of the statute with respect to insiders

---

[980] Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, p. 4 (citing a 2008 survey on attack types which ranks insider threats second only to viruses)

[981] See Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications, Vol. 2, No. 1, p. 23. See also Pfleeger, Predd, Hunker and Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions (2010), IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, p. 170

[982] Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, p. 4. Cf. the common denominator that is implicitly present in Pfleeger, Predd, Hunker and Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions (2010), IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1 and Matt Bishop and Carrie Gates: Defining the Insider Threat (2008)

affects outsider and vice versa – even though the cases are factually very different at the extreme ends of what is a scale of "insider-ness" rather than a binary state of "either or".

12.1 Defining the term "insider"

The term insider has no singular or universally accepted definition.[983] The term is used frequently in the field of IT security, especially with regards to tackling "the insider threat". However, as discussed in the chapter on problem of description, more specifically the problem with terminology, the term "insider" is not consistently given the same meaning. Rather, as has been noted by Hunker and Probst, "we are forced to conclude that the definition chosen depends on the threat of concern to the specific audience; unfortunately sometimes terminology is used without the precise definition being made clear."[984] The difficulty associated with defining who is an insider is compounded by the difficulty of defining what the perimeter is (assuming a perimeter can realistically be defined given how the internet, outsourcing and contracting etc. muddy the waters), so that a person inside the perimeter can be considered an "insider" with respect to someone outside the perimeter.[985] Furthermore, organizations are not consistent in their categorization of insiders nor do they apply a uniform approach to determining when (and in which context) a perceived attacker is categorized as an insider or outsider.[986] The meaning of the term "insider" is thus heavily dependent on the context, the system and the organization in which it is used.[987] Thus, it is arguably not appropriate to apply the organization's definition of the perimeter between the outside and the inside, its definition of "insider" in a given context and its definition of an act as an "insider threat" due to the lack of uniformity in the categorization (rendering the categorization somewhat subjective in nature and unforeseeable) and with respect to the requirement that criminal provisions be clear and precise.

---

[983] Pfleeger, Predd, Hunker, and Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions (2010), IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, p. 169

[984] Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, p. 4

[985] See Matt Bishop and Carrie Gates: Defining the Insider Threat (2008)

[986] Pfleeger, Predd, Hunker, and Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions (2010), IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, p. 169

[987] Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1, p. 5

In the IT security sector, an insider has been given many meanings; some focusing solely on anyone within the security perimeter, others any "trusted" person within the perimeter, and yet another definition focusing on those that have knowledge and privilege of the system.[988] That is, on the one hand, an outsider (e.g. a hacker) can, going by one definition, become an insider merely by crossing into the perimeter regardless of whether that person ever had legitimate access.

An insider could thus be anyone with access to materials residing within the "perimeter". Typically, an insider could be an employee, contractor or other service providers with access to systems and information belonging to others.

12.2 Insiders in US law

12.2.1 Both "insider" and "exceeding authorized access" are relative

Moreover, the term "insider" is necessarily relative. An insider cannot be an "insider" without someone having lesser privileges than the "insider" (including an entity with no privileges at all). Bishop's model of the insider is explained using an example of three users:

R_1 = "physical access"

R_2 = "physical access, user account"

R_3 = "physical access, user account, administrative privileges"

"To people who do not satisfy R_1, any person satisfying any rule is "more inside" than they, and so would be classified as an insider. Similarly, for people satisfying rule R_1 but not meeting rule R_2, any user who meets R_2 or R_3, is an insider with respect to the people meeting R_1 only. Hence being an insider is relative to some other set of people. Further, as anyone meeting R_3 also meets R_2 and R_1, and any person meeting R_2 also meets R_1, there is a natural, linear hierarchy of insiders.

More generally, let $I(R_i)$ be the set of users who have the property described in R_i. Then $I(R_1) \leq I(R_2) \leq I(R_3)$. To the members of $I(R_i)$, the members of $I(R_j)$, $i < j$, are insiders. Hence one cannot say that an entity is an "insider". Instead, one must say that the entity is an "insider with respect to the rule set R" or, when there is an inclusive relationship between the rule sets restricting two distinct entities, that one entity is an insider with respect to the other entity."[989]

The concept "insider", albeit binary in that a person is either an insider or an outsider with respect to another person with greater or lesser privilege, the concept also has linear properties. Person A,

[988] Matt Bishop and Carrie Gates: Defining the Insider Threat (2008)
[989] Matt Bishop: Position: "Insider is Relative" (2006), p. 78

who has very limited access, is an insider with respect to person B, who has no access at all. However, at the same time as A is an insider with respect to B, A is not an insider with respect to person C, who has complete access and thus is an insider with respect to both A and B. Hence, the linear hierarchy of insiders described by Bishop emerges.

Because of the pervasiveness of computing and the advent of the Internet and the World Wide Web, no one is truly an outsider with respect to publicly accessible systems because at least some access is allowed to everyone, however limited. The term "insider", if used to refer to the entire global population in the context of publicly accessible systems, thus loses its meaning because the concept's relative nature requires the existence of an entity with lesser or no privileges. The argument was thus that the term "exceeding authorized access" was not applicable with respect to ordinary users who possess no greater privilege than anyone else in the entire set of users in existence, i.e. the global population.

As described in the same chapter, the model breaks down where the courts have allowed system owners to selectively exclude a user from accessing the public website despite authorization being granted to the remainder of the global population. Allowing that to take place creates the comparative element required by Bishop's model in order for someone to be an "insider". The single user allowed to be excluded, through his "demotion" effectively "promotes" the remaining users to "insiders" with respect to himself. He (or rather the courts) thereby creates a new bottom level in the linear hierarchy where "exceeding authorized access" (the insider rule) becomes applicable to ordinary users of web servers. This would essentially lead to an inflated applicability of either "exceeding authorized access" or "without authorization" (depending on the chosen frame of reference), since only the excluded person is truly without authorization, ordinary users would owing to the "insider" concept's relative nature, "without authorization" could be applied to "insider" actions as well, since the insider's (apart from the superuser/root/administrator) action would be "without authorization" (an outsider action) with respect to a more privileged user (an insider higher up in the hierarchy). The superuser (R_3 in Bishop's example) would be incapable of exceeding authorized access, because he cannot exceed that which is unlimited.

Thus, the term "exceeding authorized access" is relative like the term insider and logically follows Bishop's model, requiring the existence of a person with lesser privilege. The Committee Reports on the CFAA, which explicitly use the terms insiders and outsiders, support the notion of relativity that lies behind the statutory language. In addition, because no one is an insider with respect to the

superuser, it follows that the superuser cannot exceed authorized access, as the term "exceeding" necessarily alludes to the possibility of attaining greater privilege (since that which is ultimate cannot be exceeded).

Perhaps it is simpler to say that the additional privileges belonging to R_2 (and not possessed by R_1) can simultaneously be seen as being (1) entirely outside the authorization of R_1, and (2) in excess of R_1's authorization. Both "without authorization" and "exceeding authorized access" can theoretically be triggered.

Because of the global-scale authorization that follows from choosing to view ordinary web site users' authorization as being based on implied consent (the basis of the authorization) it renders application of the 30 year old CFAA rather awkward, because everyone is an "insider" since they have some authorization, but it ignores the comparative element in that for the vast majority of public systems there exist no outsiders (except those few the courts have granted injunctions against).

12.2.2 Who defines "authorization"?

Bishop defines an insider based on two basic acts: (1) "violation of a security policy using legitimate access, and", (2) "violation of an access control policy by obtaining unauthorized access."[990]

However, from a criminal law perspective, it could be perceived as a weakness that the legitimacy of access and thus its counterpart, unauthorized access, is defined by the organization (that defines the policy). Because the organization is free to define what legitimate access is, it follows that they define the scope of acts covered by the criminal law prohibiting unauthorized access. Furthermore, there is a risk that whatever has been written in an organizations policy is not actually being enforced or followed in the organization; i.e. there is a risk that the enforcement of the written policy is arbitrary because the policy does not describe the practice followed in the organization.

There has been rather substantial debate among U.S. courts as to the meaning of "authorization", with the debate particularly centering on how or whether to apply the CFAA in cases where an employee had authorization to access their employer's computer but did so for a purpose that was

[990] Matt Bishop and Carrie Gates: Defining the Insider Threat (2008)

contrary to the interests of the employer or where such access was contrary to the organization's use policy. The CFAA defines "exceeding authorized access", but not "authorization" upon which the definition is reliant. 18 USC § 1030(e)(6) defines "exceeding authorized access":

"the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;"

12.2.3 Former employees

Although the majority of cases involve a person who was an employee at the time of the access, several cases involve former employees accessing their former employer's computers or computers belonging to a third-party providing access to computers to an organization's employees. For the most part, these cases do not seem to give rise to any disagreement among the courts. After all, one could argue that common sense dictates that a former employee does not retain authorization to access the organization's computers after they have left their position – even if the organization fails to disable the former employee's access credentials.

In the criminal case *United States v. Sablan*[991], the defendant had recently been fired from her position at a bank for "circumventing security procedures in retrieving files". After her being fired, Sablan went to her former place of employment, entered the building using an old key she had retained, and used an old password to gain access to the bank's mainframe. Sablan then allegedly proceeded to alter and delete several files, thereby causing damages to the bank's files. The CFAA subsection brought into play in her prosecution was (a)(5); the subsection that prohibits the intentional accessing *without authorization* and then causing damages to information. In the 1986 version of the CFAA (the applicable version at the time of Sablan's prosecution) subsection (a)(5) was squarely aimed at "outsiders" (those with no authorization to access the system).[992] It can therefore be surmised that it was undisputed that Sablan lacked any and all authorization to access her former employer's computers. Therefore, the fact that a former employee's access credentials have not been revoked by the organization and that the computer will thus grant access if those access credentials are supplied by the former employee, does not mean that the access was "authorized" within the meaning of the CFAA. That is, although the access appears authorized from a technical point of view (in that the computer is configured to grant access when valid access

[991] *United States v. Sablan*, 92 F.3d 865 (9th Cir. 1996)
[992] See Senate Report No. 99-432, at **2488

credentials are provided) that consideration does not negate or override the fact that authorization was terminated at the end of the employment.[993]

The same applies where an employee, through his employment, has had access to the computers of a third party rendering services to his employer. In *United States v. Shen*[994], a former employee of a university continued accessing the password-protected computers of a third party service provider to which he had had access in connection with his employment at the university. The court argued that "[t]here is significant authority that such access is unauthorized under §1030(a)(2)(C)". Shen argued that § 1030(a)(2)(C) was vague "as applied" to him, based on the fact that authorization to access the third party's computers had its basis in an agreement between the university and the third party. Shen had never seen the agreement and claimed that he was thus not on notice that his access was unauthorized and therefore criminal. The court responded that "[t]here is some disagreement as to whether an employee who properly accesses a computer and then misuses the information can be convicted under § 1030(a)(2)(C). However, courts are clear that employees who gain access to a computer through their employment lose authorization once they have resigned or been terminated. Moreover, persons of common intelligence would understand as much." (citations omitted)

However, the CFAA's applicability to persons accessing computers belonging to their former employers is not always so cut-and-dried. In *EF v. Explorica*, a case also discussed in connection with outsiders, a former employee was held to have accessed EF's public website in excess of his authorization. EF's website, as may be recalled, allows visitors to browse tour prices for various destinations. The abbreviations chosen by EF for gateways, destinations etc. were an element in the URL (visible to anyone in the address bar of the browser; such as BOS for Boston). EF claimed that these "codes" were proprietary and subject to the former employees confidentiality agreement. These "codes" had been used by the defendant in order to create a scraper that would allow for the automated retrieval of price information from EF's public website. Competition thus became more efficient for Explorica. The court argued that because the former employee "voluntarily entered into a broad confidentiality agreement prohibiting his disclosure of any information "which might reasonably be construed to be contrary to the interests of EF"", he then exceeded his authorization to navigate EF's public website "by providing proprietary information and know-how" to the party

[993] See also *United States v. Steele*, 595 Fed.Appx. 208 (4th Cir. 2014)
[994] *United States v. Shen*, 2015 WL 3417471 (E.D. Missouri 2015)

that created the scraper.[995] The court boldly stated that Explorica's use of the "codes" to gather prices from EF's website reeked of use and abuse of proprietary information that exceeded authorized "use" of EF's website.[996] Zefer, the third party who developed the scraper, appealed the injunction. In that case, the 1st Circuit clarified its position in the Explorica case[997], and furthermore stated that it was by no means clear that Zefer could have known that the "codes" were confidential, and that the codes could have been extracted manually had Zefer not received them from Explorica.[998]

The case, in my opinion, is particularly odd[999] in the sense that the information accessed on the website (as well as the "codes" in the URL) were publicly accessible and visible to anyone (any information obtained could equally have been obtained by any member of the public). It would seem that knowledge obtained during employment about the website's structure that would allow more efficient browsing and retrieval of information from the website can, if used contrary to agreement, incur liability under the CFAA. This would seem to apply regardless of whether such knowledge could be independently obtained by anyone by viewing the website and its URLs. For example, if A, an employee of B, has prior knowledge of the address of the location of B's apple stand and has signed a confidentiality agreement covering that information, including that A cannot use that address information in a way that is contrary to B's interests. A then quits his job with B and takes a job with B's competitor C. The new employer, C, then charges A with retrieving the prices from the signs at B's apple stand for the purposes of undercutting B's apple prices. Does it matter whether A spends extra time looking up the address of B's apple stand (which is in the

---

[995] *EF Cultural Travel v. Explorica*, 274 F.3d 577, 583 (1st Cir. 2001)
[996] *EF Cultural Travel v. Explorica*, 274 F.3d 577, 583 (1st Cir. 2001)
[997] Including its clear rejection of the district court's "reasonable expectations" test discussed earlier.
[998] *EF Cultural Travel v. Zefer*, 318 F.3d 58, 61-62 (1st Cir. 2003)
[999] Personally, I have some rather strong doubts with respect to labelling publicly visible abbreviations or acronyms as proprietary information capable of being covered by a confidentiality agreement. Especially, when determining the meaning of a "code" such as "BOS" is extraordinarily easy when it appears in the context of a travel website. The question is perhaps rather whether most people would even be interested enough in gathering these "codes" and their meaning. But lack of interest in publicly available information hardly makes the information confidential or their meaning "secret" in some way. In my opinion the 1st Circuit misses the point. The access to the information retrieved from EF's website was in no way restricted. In fact, the information was intentionally published on the World Wide Web, available to anyone, and as the court itself recognizes, EF would dislike the manual retrieval of the price information as well. The use of the supposed confidential codes was at best incidental to the access of the information, because the retrieval of the information was not predicated on a visitor supplying those codes. There is a disconnect. The codes were seemingly not originally obtained in excess of authorization to access a computer during the employment, and even if they were, knowledge and/or use of the codes is not necessary to access the public price information. They were not passwords that granted access to information to which other members of the public did not have access. Arguably, EF got lucky in that they managed to cut off their competitor's access to information available to anyone on their public website.

phonebook) just to be able to claim that he did not make use of prior knowledge, or if he immediately relies on his prior knowledge of the address? And, how then does use of the prior knowledge of the address relate to A's authority to read the prices off B's signs at the apple stand? It does not.

The Explorica case, however odd it may be, is then ostensibly a contract-based construction of "authorization" (where the contract in question does not purport to regulate access or authorization to such access), since the excess of authorization was held to derive from use of proprietary "codes" contrary to a confidentiality agreement.

In fact, "authorization" in all the cases analyzed in the context of former employees rest on a contract-based approach to construing "authorization" in the context of the CFAA. The authorization of the former employee to access the organization's computers is terminated not because the former employee's access credentials have been revoked and technical access is no longer possible, but because the employment relationship is terminated.

It would be awkward if a former employee could continue to access the organization's (non-public) computers until his access is technically revoked by a system administrator. However, it is equally awkward to construe the CFAA to cover a former employee's post-employment access to the public website of the organization where the information accessed is equally accessibly to any member of the public, irrespective of whether the former employee possessed knowledge that allowed him to do it more efficiently. He was authorized to obtain the price information. The latter begs the question: What is being protected?

12.2.4 Current employees

The application of hacking statutes to current employees is more complicated. Employees already have access and thus the attention centers not on preventing access to the "perimeter", but keeping employees from trespassing into other domains within the perimeter. For example, a person working in the HR department does not need access to the accounting system. People in assembly may need access to technical drawings, but do not need access to HR systems. Although most organizations would (and should) restrict such intradepartmental access through code, where there is no general reason for such accessibility, many organizations are equally concerned with *for what reason* an employee accesses the organizations computers and information. Similarly, organizations

may be concerned with *to what use* an employee might put the information afterwards. It is not uncommon for organizations to spell out access restrictions (including e.g. that the computers may only be used for business-related purposes) and they may also have employees sign confidentiality agreements. The question is whether a breach of use policy and confidentiality/non-disclosure agreements (or any trade secret-related agreement) can form the sole basis for criminal and/or civil liability under the CFAA.

Use policies are written by the organization. They vary in qualitative terms such as clarity and specificity. Furthermore, use policies may only be the *de jure* policy whilst the *de facto* policy may differ significantly from the former. A policy may, for example, prohibit personal use of the organization's computers. However, in practice, some personal use is clearly tolerated by the organization. Just because the organization has a use policy and that (*de jure*) use policy has been breached, it is incredibly problematic, and suspect from a due process point of view, if a court blindly enforces such a policy or punishes the breach of such a policy under a criminal statute. It should not be a foregone conclusion that criminal or civil liability has been incurred. That is, there has to be consistency between the policy on paper and the policy in practice before a court considers using such a policy to interpret "authorization". The enforcement of the policy cannot have the appearance of being arbitrary or contrary to the organization's *de facto* practice.

12.2.4.1 Agency-based approach

The agency-approach is based on the rather vague concepts of loyalty and adverse interest as well as the questions that relate to the very existence of an agency relationship (which under some circumstances can be formed without the employee's knowledge) the approach is understandably very favorable to employers seeking to punish disloyal employees.[1000]

In *Shurgard v. Safeguard*[1001] the parties were competitors in the self-storage business. Shurgard had filed suit against Safeguard because several of Shurgard's employees had allegedly accessed its computers to send trade secrets to Safeguard, who subsequently hired those employees. At the time

[1000] See Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819, 824 ("Notable as well is the fact that this agency-based interpretation is undoubtedly the most employer-favorable approach, since simply characterizing the employee's actions as against the employer's interests will likely result in liability." Field further points out that the 7th Circuit's acceptance of the agency approach appeared to increase the number of companies filing claims under the CFAA.)
[1001] *Shurgard v. Safeguard*, 119 F.Supp.3d 1121 (W.D. Wash. 2000)

of their access to Shurgard's computers, the employees had had full authorization to access the information in question. Therefore, in order to state a claim under the CFAA, the Shurgard had to show that the employees, despite the apparent authorization, were not authorized to access the computers. To do so, Shurgard relied on Restatement (Second) of Agency § 112 (1958) and claimed that the employees had acquired adverse interests the effect of which was an automatic termination of authorization. Under Shurgard's theory, the employees had lost their authorization when they accessed the computers for the purpose of sending trade secrets to Safeguard; a purpose that did not further the interests of Shurgard. The court agreed, and held that Shurgard had stated a claim under the CFAA.

The cessation-of-agency theory gained some traction when the Seventh Circuit rendered its decision in *International Airport Centers v. Citrin*[1002]. Jacob Citrin had decided to quit his job at IAC and start his own business. This constituted a breach of his employment contract with IAC. Furthermore, before Citrin returned his company-issued laptop, he erased all the data on it, and to prevent the recovery of the data, he ran a "secure-erasure" program that overwrote the files. The court had the unenviable task of determining whether Citrin had authorization to access the computer and destroy the files.[1003] The court looked to *Shurgard* and the Restatement (Second) of Agency §§ 112 and 387 (1958), and argued that Citrin's deletion of the files was "in violation of the duty of loyalty that agency law imposes on an employee."[1004] The court thus concluded that Citrin's authorization had been terminated, and his deletion of files was "without authorization", as opposed to in "excess of authorization".[1005]

The Seventh Circuit's formal adoption of the cessation-of-agency in the context of applying the CFAA to disloyal employees started an, at times, heated debate between the appellate courts, effectively dividing them in their approach to construing authorization under the CFAA, and even dividing the lower courts within circuits that had not yet addressed the applicability of the CFAA in this context. The agency-based approach has also attracted criticism from commentators.[1006]

[1002] *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006)
[1003] Curiously, it appears that Citrin's employment contract explicitly permitted him to "return or destroy" data on the laptop at the end of employment. The court proceeds to guess as to the purpose of such a contract clause arguing that the purpose could not have extended to Citrin's decision to delete files. See *Citrin*, at 421.
[1004] *Citrin, at 420*
[1005] *Citrin*, at 420-421
[1006] See e.g. Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819 and Orin S. Kerr: Cybercrime's Scope: Interpreting

It appears that no other appellate court has fully agreed to follow the very broad interpretation of "authorization" inherent in the Seventh Circuit's agency approach, although not for the lack of plaintiffs attempting to rely on the agency theory in *Citrin* in other jurisdictions; after all, the agency theory is very employer-friendly, since the fluid concept of disloyalty suffices to state a CFAA claim[1007]. Several lower courts within other circuits subscribed to the agency theory.[1008] Even though other appellate courts have not adopted the Seventh Circuit's line of thinking entirely, that does not mean that the courts have generally discounted broad interpretations of "authorization" either, particularly where the purpose with which the employee accessed the computers was contrary to the organization's computer use policy and where that policy was known to the employee. That is, the cases are more grounded in a slightly less broad approach based on contractual obligations.

12.2.4.2 Contract-based approach

Even though the agency approach is a kind of variant of a contract-based approach, the agency approach is focused on the special duties (namely, loyalty) that follow from the nature of the employer-employee relationship, rather than being an approach applicable to all contracts in general. Whereas the plaintiff, under the agency-based approach, need not specify any access restrictions as the lack of authorization is rooted in "disloyalty", the contract-based approach requires there be a contract that regulates access and that the defendant accessed the computer in violation of that contract. This approach has been applied with respect to both employees (insiders) as well as outsiders.

United States v. Czubinski[1009], a case before the First Circuit court, concerned the act of an employee of the Internal Revenue Service (IRS). Czubinski had a valid password to access any taxpayer's income tax return information. The IRS' rules of conduct, of which Czubinski had acknowledged his receipt and which he had signed, clearly prohibited employees from accessing the files outside the course of his official duties. Czubinski had searched the database on several occasions and looked at taxpayer information without there being an official purpose for doing so.

'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU L. Rev., Vol. 78, No. 5, pp. 1596-1668 (the article predates Citrin, but comments on the agency-approach in Shurgard as being "strikingly broad")

[1007] In addition to one the prerequisites for stating a civil claim under the CFAA.

[1008] See e.g. *ViChip v. Lee*, 438 F.Supp.2d 1087 (N.D. Cal. 2006)

[1009] *United States v. Czubinski*, 106 F.3d 1069 (1st Cir. 1997)

The First Circuit stated that Czubinski had "unquestionably exceeded authorized access to a Federal interest computer."[1010] The court, however, did not explain its interpretation of "authorization", nor did it need to, because the government had charged Czubinski under subsection (a)(4) which requires that the prosecution prove that Czubinski had the additional scienter of intent to defraud as and that he had obtained "anything of value" in furtherance of the fraudulent scheme. Since the court found that Czubinski had done no more than satisfy idle curiosity and that the information obtained did not constitute "anything of value", the court reversed Czubinski's conviction without needing to explain its understanding of "authorization". The First Circuit court can at least be said to have hinted at the acceptance contract-approach, in that the court's opinion intimates that a contract, such as the IRS rules of conduct, can stipulate the scope of authorization and that such a contractually defined scope may form the basis of a CFAA claim or prosecution.[1011]

The Fifth Circuit addressed the interpretation of authorization in an employee context in *United States v. John*[1012]. John was an account manager at Citigroup and had access to the company's "internal computer system and customer account information contained in it." She had supplied her half-brother with the customer account information of 76 corporate customer accounts, and he then incurred fraudulent charges to four of the accounts. John had provided him the information by accessing and then printing the information from Citigroup's computers. She was charged with, amongst other things, exceeding authorized access to a protected computer in violation of subsections (a)(2)(A)[1013] and (a)(2)(C). In her appeal to the Fifth Circuit, John proffered the argument that she was authorized to view and print the information, and furthermore, that the CFAA did not prohibit unlawful *use* of the information she had been authorized to *access*. The court argued that the *use* of information that a person is permitted to access may be covered by "authorization", "at least, when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime."[1014] Furthermore, the court averred that using Citigroup's computers "to

---

[1010] *United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997)
[1011] See similarly Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819, 828
[1012] *United States v. John*, 597 F.3d 263 (5th Cir. 2010)
[1013] (a)(2)(A) is a subsection of the CFAA that pertains to unauthorized access to a computer and obtaining information in a financial record of a financial institution, or of a card issuer, or information contained in a file of a consumer reporting agency on a consumer. (a)(2)(C) is aimed at information on a protected computer in general, rather than specific types of computers and information.
[1014] *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010)

perpetrate fraud was not an intended use of that system."[1015] Moreover, John's use of the computer was in violation of a use her employer's employee policy – a policy of which John had knowledge. The policy, which John had been taught about during training programs, prohibited misuse of Citigroup's systems and misuse of customer information. In an effort to substantiate that such a policy could delineate the scope of authorization, the court cited *EF Cultural Travel v. Explorica* – albeit, explicitly disagreeing with the First Circuit's holding that a confidentiality agreement under the circumstances in *Explorica* could form a basis for a CFAA claim – agreeing with the First Circuit's argument that "exceeding authorized access" may include "exceeding the purposes for which access is "authorized." Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded."[1016]

The Fifth Circuit's explanation of its disagreement with the First Circuit's holding in *Explorica* that a confidentiality agreement could define limit access authorization and thus create criminal liability under those circumstances reveals that the John court may have misunderstood the underlying facts of the Explorica case – or perhaps rather, the John court inadvertently relied on the Explorica court's ostensibly faulty logic and arguably misguided application of the CFAA. The First Circuit's "authorization limited by purpose" argument in Explorica had, in fact, nothing to do with the defendant's purpose of accessing EF's website or the purpose of the defendant's use of the information accessed (that is, the accessed price information on the public website). The Explorica case involved a very broad confidentiality contract that forbade *disclosing* any information that might be construed contrary to the interests of EF Cultural. The agreement therefore had nothing to do with regulating the *authorization to access* the publicly accessible price information or EF's public website, nor did it more generally regulate the use of, any publicly accessible information (such as EF's online prices) or the use of publicly accessible computers owned by EF Cultural Travel. In fact, the confidentiality agreement could impossibly have covered the price information available on a public website, because that information could not in any plausible way be construed as confidential or proprietary. In other words, access to the price information on EF's website was completely unrestricted. Why a breach of such a confidentiality agreement was allowed to regulate authorization under the CFAA when the agreement did not relate to any access restrictions to the information on the website in question is nothing short of confounding. Thus, not only is the First Circuit's construction of "authorization" not appropriate in a criminal context, it is inappropriate in any context. However, in *John* there is no such disconnect between the agreement, the access and the information obtained. The employee policy directly targeted the limitation on use at the information that John accessed and subsequently misused. Notwithstanding that the Fifth Circuit's deference to *EF v. Explorica* is arguably misguided and Explorica fails to lend persuasive authority to the Fifth Circuit's "access limited to certain purposes through contract"-argument in John, the theory is not necessarily without

[1015] *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010). The "intended use" is a reference to the Second Circuit's "intended function" argument in *United States v. Morris*. The Fifth Circuit had cited the argument in an earlier case, *United States v. Phillips*. However, the original "intended function" test proffered by the Second Circuit differs from the Fifth Circuit's "intended use" in *John*. In *Morris*, the defendant had exploited vulnerabilities in system utilities that he had access to and used that exploit to spread a worm on the early Internet.
[1016] *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010)

merit for that reason alone. It depends on whether "purpose of access/use" comports with the language of the CFAA. Thus, I am not discounting the Fifth Circuit's reasoning simply because their reliance on Explorica, in my opinion, is misguided.

According to the policy, John had not been authorized to access Citigroup's systems for all conceivable purposes, but for a limited purposes only. John acted in contradiction to the policies that applied to her as an employee of Citigroup. The court concluded that since John knew that she accessed the information on the computer in violation of Citigroup's employee policy and as a part of a criminal scheme, her conduct exceeded authorized access within the meaning of § 1030(a)(2).[1017] The court used that same reasoning to distinguish *John* from the Ninth Circuit's decision in *Brekka* in which the Ninth Circuit construed the CFAA narrowly in a civil case in light of the rule of lenity. Due to John's knowledge of her violation of the policy and her participation in a criminal scheme, the Fifth Circuit intimated that the rule of lenity need not be considered.[1018]

Although the *John* decision does not include verbatim excerpts from the Citigroup policy she apparently violated, it is arguably safe to assume that even if the policy used a broad and malleable word like "misuse" with respect to its systems and confidential customer information, it is similarly safe to qualify the use of the customer information to incur fraudulent charges as "misuse". However, "misuse" of Citigroup's systems is much broader than "misuse" of information. The logical temporal order of the events relevant to the CFAA dictates that misuse of information can only occur *after* the information has been obtained through use of the systems (whether it be use or misuse). Solely obtaining the information alludes to nothing about any subsequent events. It alludes only to knowledge, viewing, and perhaps retrieval, of the information, whereas use or misuse of the information implies that the information has, at least, been – at the risk of "sounding" redundant – put to use. Temporally, *use* of information not only comes after *accessing* them, but *use* also comes after *obtaining* the information. The CFAA declares no rules relevant to events involving the information after they have been obtained. Of course, one could argue that (a)(4) involves purpose of access or use of information, because the subsection requires an additional scienter of intent to defraud and that the unauthorized access or exceeding authorized access furthers a fraudulent scheme. However, such an argument fails, because such a reading of (a)(4) would make both "unauthorized" and "exceeding authorized" superfluous, since any access then, regardless of whether it is authorized or not, would violate (a)(4) so long as the access is done with intent to defraud.

The Eleventh Circuit has also weighed in on the interpretation of authorization in the employee context. In *United States v. Rodriguez*[1019], the defendant, an employee of the Social Security Administration, had accessed and obtained a relatively wide range of personal information regarding 17 people he knew to various extents. He was charged with exceeding authorized access

[1017] *United States v. John*, 597 F.3d 263, 273 (5th Cir. 2010)
[1018] *United States v. John*, 597 F.3d 263, 273 (5th Cir. 2010)
[1019] *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010)

in violation of § 1030(a)(2)(B)[1020], the subsection specifically aimed at information obtained from any department or agency of the United States. The Administration had a clear policy prohibiting obtaining information from the Administration's databases for non-work related reasons. In fact, employees were informed about that policy through mandatory training, notice signs around the office, and a warning banner on the computer screens on a daily basis. Furthermore, Rodriguez, like the other employees, had renew his commitment to the policy on an annual basis by attaching his signature to a form acknowledging the receipt of the policy. The policy included a warning that a violation would incur criminal liability. For three consecutive years, Rodriguez refused to sign for the receipt of the policy. During trial, Rodriguez admitted that he had accessed information without authorization. However, in his appeal to the Eleventh Circuit, Rodriguez attempted to rely on *Brekka*, claiming that the only databases he accessed were the ones he was authorized to access. However, the Eleventh Circuit distinguished Rodriguez' case from Brekka in that whereas there was no policy regulating Brekka's use and there was no dispute as to Brekka's authorization to access the documents in question, Rodriguez's access had been subject to the Administration's employee policy that limited the authorization to access for business reasons only and Rodriguez had conceded at trial that he did not access the information in question for business reasons. Thus, under the Eleventh Circuit's theory, Rodriguez' authorized access was converted to unauthorized access ("exceeding authorized access"), because the access was in violation of his employer's policy.[1021]

12.2.4.3 Code-based approach

So far, the two broader approaches to interpreting "authorization" in the employee context have been accounted for. The broadest, the agency-based approach having been accepted by the Seventh Circuit, and the less broad contract-based approach having been accepted in the First, Fifth and Eleventh Circuits.

[1020] See also *United States v. Teague*, 646 F.3d 1119 (8th Cir. 2011). *Teague* also involved access to personal information residing in a government database. Teague had access through her job at a company contracted by the government to collect debts (student loans) and generally answer questions related to student loans. It seems Teague did not dispute the claimed lack of authorization. Rather she claimed that someone else had used her access credentials. The court thus never engages in an analysis of the meaning of "authorization", even though it states that lack of authorization must be proved by the government. The decision, however, only discusses efforts made to prove that Teague was indeed the person using her access credentials at the time of access, not whether her access was subject to any policies regarding non-business use etc.

[1021] See also Audra A. Dial and John M. Moye: The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft? (2013), 64 Hastings L.J. 1447

The narrow code-based approach essentially involves *not* reading "use" or "purpose" into the language of the CFAA. Although, the approach is called "code-based", the approach, in its purest form, cannot reconcile cases where the code-based approach is reasonably warranted in light of notice (foreseeability) issues and those cases where e.g. a janitor (who is also an employee and also a type of insider) has physical access to an unprotected computer in the course of his building maintenance duties. Nor is the approach as applied by the courts truly "code-based", but rather, those courts are rejecting the contract and agency-based approaches. The Fourth and Ninth Circuits have accepted this approach. The Second, Third[1022], Sixth, Eighth and Tenth Circuit Courts have yet to explicitly adopt an approach. The Second Circuit may have implicitly adopted the narrow approach.[1023]

The Ninth Circuit adopted the narrow approach in its decision in *Brekka*[1024] and in *United States v. Nosal*[1025]. In *Brekka*, the defendant had been hired by LVRC, a treatment center for addicted persons, in part to conduct internet marketing and interacting with a third party service provider retained by LVRC to provide email service, website services etc. LVRC and Brekka did not have a written employment agreement, nor was there any employee policy regarding Brekka's use of the computer. Since Brekka resided out-of-state and had to commute to back and forth between the treatment center and his home, Brekka had emailed himself some documents that related to his work for LVRC and documents that related to earlier negotiations with LVRC regarding Brekka purchasing an ownership interest in the center in order to access them on his own computer. When Brekka later resigned, he left his computer at LVRC without deleting anything from it. Upon discovering that Brekka had emailed himself work-related documents, LVRC brought action against Brekka under the CFAA[1026] claiming that Brekka's authorization had ceased when he used the computer contrary to LVRC's interests[1027].[1028] The court did not agree with LVRC's perception of

---

[1022] The two dissenting judges in *Nosal* aver that the Third Circuit has implicitly adopted the Fifth and Eleventh Circuits' reasoning. However, the judges, regrettably, do not provide any case citations to substantiate that assertion.
[1023] *Nexans Wires, S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559, 563 (2nd Cir. 2006). See *JBCHoldings v. Pakter*, 931 F.Supp.2d 514, 524 (S.D.N.Y. 2013). The lower courts in the Second Circuit are split at the moment. See also e.g. *United States v. Valle*, 301 F.R.D. 53 (S.D.N.Y. 2014)
[1024] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)
[1025] *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012)
[1026] § 1030(a)(2) and (a)(4)
[1027] I.e. LVRC relied on the Seventh Circuit's agency-based interpretation of authorization in *Citrin*.
[1028] *Brekka* also involved alleged unauthorized access after Brekka's employment ended. However, that allegation was not proven in court and so I omit reference to it to minimize any distraction from the central point of the narrow approach fully adopted by the Ninth Circuit in *Nosal*, the adoption of which relied on the outcome of *Brekka*. In the court's summary of facts relevant to the case, there is mention of Brekka's owning two consulting businesses whose

authorization. The court's opinion was rooted in the plain meaning of the statute, the language of which, the court found, did not support the agency-based approach to interpreting "authorization". The court's reasoning was that for the purposes of the CFAA, an employee who has been granted authorization to use a computer "subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations."[1029] The court argued that this resulted in a more sensible interpretation of the "without authorization" and "exceeding authorization" dilemma, because a person without authorization to access a computer, has no permission to use the computer at all, whereas a person that has permission to access the computer but who accesses information they are not entitled to access exceed their authorization. One lacks any and all authorization to access the computer whereas the latter has authorization to access the computer but is only authorized to access some, but not all, information on that computer. Thus, entirely lacking authorization to access the *computer* differs from being authorized to access the computer but entirely lacking authorization to access certain *information*. It is thus not a question of what the person does with the information he is entitled to access, rather whether one was entitled to access the information - period. Thus, in *Brekka*, the Ninth Circuit refused to adopt the agency-based interpretation on the grounds that it did not comport with the plain language of the statute, and given the fact that the CFAA is a criminal statute, also rejected the approach on lenity[1030] grounds.

Certain passages in *Brekka* might have given plaintiffs and the government reason to assume that the existence of a policy regulating for what purposes information could be accessed and a violation of that policy could suffice to state a claim under the CFAA.[1031] However, the Ninth Circuit set the record straight in *United States v. Nosal*[1032]. The Ninth Circuit's decision in *Brekka* was rendered at a time when another employee, albeit caught up in a CFAA criminal case[1033], had just been denied

---

operations included referral of potential patients to rehabilitation centers. The decision mentions only the plaintiff's allegation of access to further his own personal interests.

[1029] *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)

[1030] I discussed the rule of lenity above in the chapter on nullum crimen sine lege. *Brekka* is arguably one of those cases where the rule of lenity is cited only in order to bolster a conclusion that has already been reached. Here, the Ninth Circuit, had already concluded that the agency theory is not supported by the plain language of the statute. Arguably, the court either only pays lip service to the rule of lenity in that it has already rejected the agency theory, or this may or may not be a reference to that the agency-based construction might have been acceptable had it not been proffered in the context of a criminal statute. The latter of course is speculative.

[1031] The *Brekka* court specifically mentioned the absence of an employee policy with respect to computer use.

[1032] *United States v. Nosal*, 676 F.3d 854 (9th Cir. (en banc) 2012)

[1033] Nosal, a former employee, had been charged under (a)(4) for aiding and abetting current employees in exceeding their authorized access with intent to defraud.

the dismissal of his CFAA charges. The Ninth Circuit court, thus, granted Nosal a rehearing en banc.

The government's interpretation of "exceeding authorized access" was that a company computer use policy gives employees certain rights, and employees that violated the policy exceeded their authorized access. The court disagreed and explained that "entitled" in the statutory definition of "exceeding authorized access" "refers to how an accesser "obtain[s] or alter[s]" the information, whereas the computer use policy uses "entitled" to limit how the information is used after it is obtained. This is a poor fit with the statutory language. An equally and more sensible reading of "entitled" is as a synonym of "authorized." So read, "exceeds authorized access" would refer to data or files on a computer that one is not authorized to access."[1034] (citations omitted)

Similar to my argument above in connection with *United States v. John*, the Ninth Circuit points out in a footnote that the government's proposed construction of "exceeds authorized access" in *Nosal* renders the entire "intent to defraud" element in (a)(4) superfluous, because using a computer with intent to defraud necessarily violates company policy.[1035] To that one can safely add that that conclusion is even more certain with respect to the agency-based approach, which relies on the agent acquiring adverse interests.

The government's theory, according to the court, would expand the CFAA and criminalize "any authorized use of information obtained from a computer."[1036] Furthermore, the government's assertion that the defendant was on notice that his act was wrongful *because* it was fraudulent and the access furthered the fraud (i.e. Nosal was supposedly on notice that the former employees' access was unauthorized under § 1030(a)(4) because the access furthered a fraudulent scheme – that is, the government effectively eliminates the need for the term "unauthorized"; an essential element of the statute) ignored that "exceeds authorized access" is used elsewhere in the CFAA. For example in § 1030(a)(2), which requires no fraudulent intent. If an intent to defraud in itself negates authorization to access then (a)(4), which specifically requires an intent to defraud, would be entirely superfluous.[1037]

[1034] *United States v. Nosal*, 676 F.3d 854 (9th Cir. (en banc) 2012)
[1035] *United States v. Nosal*, 676 F.3d 854, 858 (FN4) (9th Cir. (en banc) 2012)
[1036] *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. (en banc) 2012)
[1037] The government suggested that the court's construction should then only apply to (a)(4). The court rejected this proposition stating that "[g]iving a different interpretation to each [instance of "exceeds authorized access" in the CFAA] is impossible because Congress provided a *single* definition of "exceeds authorized access" for all iterations of the statutory phrase." *Nosal* at *859 See also Stephanie Greene and Christine Neylon O'Brien: Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act (2013), 50 Am. Bus. L.J. 281

Of further concern to the court was that the government's proposed construction "allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law" whereas those relationships would normally be regulated by tort and contract law.[1038] [1039] The court furthermore looks to the consequences of yielding to the government's argument. If private use policies can dictate the meaning of "authorization" in the context of the CFAA, that will not only effect employees, but any internet user who interacts with computers the use of which is subject to terms of service or terms use. That is, the consequences of recognizing private policies as limitations on authorization (in the meaning of criminal statute) will affect the construction of authorization also with respect to "outsiders"; not just employee cases and not just in the case before the court. The court did not accept, either, the government's assurances that it would not pursue minor violations under the CFAA. To that promise it responded: "[…][W]e shouldn't have to live at the mercy of our local prosecutor."[1040] The Ninth Circuit said of its sister circuits that had adopted the contract-based approach and the agency-based approach, that "[t]hese courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access.""[1041] And so, the court concluded that if Congress wanted to include liability for misappropriation into the CFAA it would have to do so more clearly. Until then, lenity would prevail.[1042] The CFAA's concept "exceeds authorized access" prohibits unauthorized access to information, not the unauthorized use thereof.[1043]

The Fourth Circuit followed in the Ninth Circuit's footsteps and adopted the narrow code-based approach in *WEC v. Miller*[1044]. Shortly before Miller resigned from his position with WEC, WEC alleged that Miller and his assistant had downloaded proprietary and confidential information from

---

[1038] *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. (en banc) 2012)
[1039] The court specifically cited *Lee v. PMSI*, 2011 WL 1742028 (M.D. Fla. 2011) in which a pregnant woman had been fired. She sued for pregnancy discrimination and her former employer countersued under § 1030(a)(2)(C) arguing she had used company computers excessively for personal reasons such as checking email, Facebook and news. The claim was dismissed, because the statutory language as well as the spirit of the CFAA did not support the claim. (Legislative history makes it clear that such personal use falls outside the scope of the CFAA. See H.R. Report 98-894 at **3708.) The *Nosal* court notes that although a company is able to fire employees for violation of computer use policies that is quite different from make such a violation a criminal offense. See *Nosal* at 860, FN7.
[1040] *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. (en banc) 2012)
[1041] *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. (en banc) 2012)
[1042] Again, the court had arguably already arrived at its decision, since it had already stated that the contract and agency approaches were incompatible with the statutory language. Thus, there was no tie for the rule of lenity to break, because in the court's view, there was only one plausible construction.
[1043] *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. (en banc) 2012)
[1044] *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012)

WEC's computers[1045], and used that information to make a presentation to a potential customer on behalf of WEC's competitor, Arc[1046]. WEC had promulgated policies prohibiting unauthorized use of information or downloading the information to a personal computer. The policy did not regulate access to information.

Not surprisingly, at trial, WEC relied on *Citrin* and claimed that by violating the use policy, the defendant had breached his fiduciary duties to WEC and that breach meant that Miller had lost his authorization to access the information or he had exceeded his authorization by accessing the information.[1047] In other words, WEC argued that Miller had become an agent of Arc.[1048] On appeal, WEC relied on the earlier Ninth Circuit panel decision in *Nosal*, which had, however, been reversed en banc, arguing that the policy described the manner in which employees were allowed to access, and that the defendant had violated that policy.

The court framed the question before it as a question of whether the terms "without authorization" and "exceeds authorized access" extended to violations of information/computer use policies. It concluded that it did not. The Fourth Circuit discussed both the Seventh Circuit's agency approach and the Ninth Circuit's narrow approach, and opted for the latter because Congress had not clearly criminalized the unauthorized "manner" of obtaining or altering information as claimed by WEC. The court cited lenity as a reason to choose the narrower approach. In completely rejecting the Seventh Circuit's agency-based approach, the *WEC* court acknowledged that Citrin's behavior had been "egregious" and that Citrin clearly violated his duty of loyalty. However, the Fourth Circuit believed that the consequences of adopting such an approach in the context of the CFAA would have "far-reaching effects unintended by Congress."[1049]

This chapter began with an attempt to show the diversity of the people who could be considered insiders; the people who have physical access to the computers (e.g. a janitor or other people allowed in the room where the computer is), the people who are authorized to access the computer logically (using the computer is a part of their job), the people who have legitimate remote access to the computer, and the people who have gained illegitimate access to the computer and are

[1045] Miller's assistant had also emailed documents to Miller's personal email address.
[1046] The customer ended up doing business with Arc rather then WEC.
[1047] On appeal, WEC relied on the earlier Ninth Circuit panel decision in *Nosal*, which subsequently had been reversed en banc.
[1048] WEC alleged violations of § 1030(a)(2)(C), (a)(4), (a)(5)(B) and (a)(5)(C).
[1049] *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012)

masquerading as a legitimate user and can do everything a legitimate user can do. The masquerader, although some may include it in the definition of insider for risk assessment purposes, is not appropriate in a legal context, but some situations may muddy the waters. Some situations fall outside all, or some, of the approaches to construe authorization because all the theories have various weaknesses.

The agency-based approach is only applicable in an employer-employee relationship. The contract-based approach only makes sense where there is a contract of some sort, and even then, it gives cause for concern to enforce every clause of every contract in every situation. Contracts (including policies) can range from the very vague to the very specific. Even assuming the contract is sufficiently specific, it raises the question whether the particular clause that has been violated, is a clause that should be enforced by threat of criminal punishment rather being subject to civil liability. Computer owners can put anything in their computer use policies and make the access authorization contingent on observance of any kind of rule; for example, if authorization to access the computer, programs or information on it, were contingent on that access being work-related, everything from whether you emailed your spouse from your work email address to using the computer to access and email trade secrets. Even though the latter is clearly deserving of some kind of punishment (in fact, the legislature has already thought of that by enacting misappropriation provisions criminalizing misappropriation!), it is worth remembering that allowing violation of computer use policies to trigger criminal liability in the "trade secret stealing" end of the scale of unacceptable behavior, also affects the other end of the scale because the emailing of a spouse contrary to computer use policy requiring a work-related purpose for access is equally a violation of policy. Either policies are considered a source of limitation of authorization in the context of hacking statutes, or they are not. In for a dime, in for a dollar. Picking and choosing whether violation of an organization's computer use policy is appropriate to enforce under a hacking statute based on the particular conduct of the defendant before the court invites arbitrary decisions, because the court would be hard-pressed to distinguish between the two previously mentioned examples where a clear policy exists prohibiting the defendant's use of the computer in both cases. The authorization to access the computers would be equally absent in both cases, if the access was for "non-business reasons". The law would not distinguish between the two in terms of determining guilt. Both the person misappropriating trade secrets and the person emailing his wife would have accessed a computer contrary to policy and lacked authorization. Only the sentencing phase would

take into account the differences between using a computer to email your spouse contrary to policy and emailing trade secrets to a competitor contrary to policy.

Allowing contracts to define and/or limit authorization in the context of hacking statutes arguably means allowing contracts to dictate the scope of "authorization" in hacking statutes in all cases. Not just insider cases, but outsider cases as well. After all, "exceeds authorization", which typically is applied to insiders, hinges on the definition of "authorization". In order to figure out whether authorization has been exceeded, one must first know what authorization is. Authorization can be delegated via contract. In terms of public websites, for example, the distinction between insider and outsider becomes obfuscated. As discussed in the chapter on outsiders, particularly in terms of public websites, an implied authorization to access a public website is presumed. In turn that means that someone accessing a public website is not entirely without authorization. Furthermore, allowing contracts to define the limits of the authorization would mean that website terms of use and terms of service could define the authorization within the context of hacking statutes.[1050]

Although employers are particularly vulnerable to employee misbehavior when the employer authorizes an employee to access computer and information, the price for including the employer's computer use policy within "authorization" or "exceeds authorization" is high, especially in light of the fact that trade secret law already provides criminal law protection for aggrieved employers.[1051]

Rodriguez and *John* both involved access to information that is specifically protected under the CFAA. In the case of *Rodriguez*, the defendant had accessed the government databases of the Social Security Administration (§ 1030(a)(2)(B)), and in *John*, the defendant had accessed the records of a financial institution (§ 1030(a)(2)(A)). When the facts of the cases are viewed in isolation, it is tempting to conclude that of course should the defendants be punished. John, because she used the information she had authorization to access as a part of fraudulent scheme. Rodriguez because he used the information gathered from the government database to ostensibly do background checks on women he was romantically interested in, e.g. showing up at their address without them having given him their address. In *United States v. Sablan*, an employee had looked up President Obama in the Department of Education's student loan database to which she had access.[1052] In short, the cases

[1050] See chapter on authorization with respect to outsiders.
[1051] In Danish law there is already a provision in the Marketing Act (§ 19) that provides for criminal liability for unauthorized access to and/or disclosure of trade secrets.
[1052] Sablan did not argue that she had authorization, but that she was not the one who had done the searches. The court never analyzes "authorization".

are not lacking unethical behavior. The question is whether the costs associated with accepting a contract-based construction of "authorization" and "exceeds authorization" are acceptable. The *Nosal* court discussed this issue at length, citing several terms of use/service agreements from various websites, such as Google and Yahoo! and gave examples of behavior that would become criminal. As may be recalled, in *Nosal*, the government stated that it would not use its prosecutorial discretion to prosecute minor violations regardless of the scope of the CFAA. However, only three years prior to *Nosal*, the government did the exact opposite in *United States v. Drew*[1053]. Drew had bullied a 13-year-old schoolmate of her daughter's on MySpace whilst pretending to be a sixteen-year-old boy whose name and photograph she had used without permission. Tragically, the girl committed suicide. Presumably as it is extremely hard to prove beyond a reasonable doubt that a person has caused another person to commit suicide, the government used § 1030(a)(2)(C) as what can best be described as a "proxy" charge. The government averred that Drew had accessed MySpace without authorization or by exceeding her authorization, because she had consciously breached the MySpace terms of service.[1054] Although the jury convicted Drew, the court subsequently granted a motion to dismiss the indictment on the grounds of unconstitutional vagueness (as applied).[1055]

As may be recalled from the chapter on nullum crimen sine lege, the void-for-vagueness doctrine is essentially two-pronged. First, there must be sufficient notice of an act being criminal. Second, the law must give minimal guidance to those enforcing the law, so that the law's enforcement is not capricious and arbitrary. The *Drew* court explained why it held that letting website terms of service define the scope of authorization in the context of the CFAA failed both prongs, although primarily it failed the minimal guidelines prong.

As to notice, first, the court stated that breaches of contract do generally not incur criminal liability. Whereas people might expect civil liability, they would not expect criminal liability – particularly noting that all breach of terms of service cases have been civil cases, not criminal.[1056] Second, the court stated that if terms of service were allowed to govern what is "unauthorized" and "exceeds authorization", which then determines whether a person has committed a crime under the CFAA,

---

[1053] *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). The case is discussed in the chapter on outsiders.
[1054] The government added that she had done so in furtherance of the tortious act of intentionally inflicting emotional distress.
[1055] See more in Orin S. Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota Law Review 1561. Available at https://ssrn.com/abstract=1527187.
[1056] *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009) and FN24

"would be unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will."[1057] "If *any* violation of *any* term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but it would, in turn, render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement."[1058] Third, the court stated that allowing terms of service to constitute a basis for a CFAA crime, "that approach makes the website owner-in essence-the party who ultimately defines the criminal conduct. This will lead to further vagueness problems."[1059] The court was concerned with the fact that the terms of service themselves may be so vague that a website visitor would not reasonably be able to understand what the terms of service encompass, such as what the prohibition against "unfair content" might mean in the MySpace terms of service, the meaning of which would be unilaterally be determined by MySpace. The court also pointed out that a breach of contract does not necessarily discharge the contract.[1060]

With respect to minimal guidelines to law enforcement, the court essentially argues that the breadth of the terms of service become the breadth of the criminalization. Lying about one's weight and age would constitute a breach under the MySpace terms of service, and so would advertising a product.[1061] People who are helping their kids who are younger than thirteen open a Facebook account might then be aiding their child in committing a crime since such conduct is contrary to Facebook's terms of service.[1062] Such overbreadth raises the question "whether Congress has "establish[ed] minimal guidelines to govern law enforcement.""[1063] Letting website terms of service govern what is authorized in terms of the CFAA would create a "standardless sweep" that would enable federal law enforcement entities to be "improperly free to "pursue their personal predilections.""[1064]

Granted, the *Drew* court was addressing vagueness introduced into the CFAA by contracts in terms of accounts on public websites. However, company use policies are not necessarily much clearer

[1057] *United States v. Drew*, 259 F.R.D. 449, 464 (C.D. Cal. 2009)
[1058] *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009)
[1059] *United States v. Drew*, 259 F.R.D. 449, 465 (C.D. Cal. 2009)
[1060] At least not in California law, which was the contract law applicable in the case. Similarly, in Danish law, a breach of contract does not automatically discharge the contract either.
[1061] See the court's numerous examples in *United States v. Drew*, 259 F.R.D. 449, 466 (C.D. Cal. 2009)
[1062] See Facebook's terms here: https://www.facebook.com/legal/terms at §§ 3.11 and 4.5. Note that in § 14 it is stated that even violating the "spirit" of the terms of service will terminate the contract.
[1063] *United States v. Drew*, 259 F.R.D. 449, 466 (C.D. Cal. 2009)
[1064] *United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (citing *Kolender*)

and narrower than then terms of service on a public website. What is more is that the company culture might be such that the policies are disregarded or workarounds for security protocols defined in the policy have become commonplace. Such a culture cannot "breed internally" in the same way between thousands or millions of website users and a website owner as it can between employees and management in an organization.

In other words, like in the outsider cases, these approaches that have been applied in the insider cases are not really working. The code-based approach arguably works, because it is not so much a code-based approach in reality, but rather a rejection of the very broad contract-based and agency-based approaches. The Fourth and Ninth Circuit are applying narrower approaches, but they have really only said what they do not think should be used to construe authorization in a criminal statute. If only a code-based approach were left, then it would be an implicit acceptance of the code-based approach. However, note that the Ninth Circuit in *Brekka*, regarding the plaintiff's claim that Brekka accessed the admin interface of the company's website statistics service after his employment ended, states that such access would have been unauthorized under the CFAA.[1065] The plaintiff failed to prove that Brekka had accessed the admin interface, but that does not change the court's point that such access would, had it been proven, fallen within the scope of the CFAA's "without authorization" concept. A true code-based approach would have held such access outside the scope of "without authorization" if Brekka had gained access using a still-active login name and password. "Code" cannot account for the court's argument.[1066]

12.2.5 Social norms-based approach

The conclusion in the chapter on authorization with respect to outsiders (primarily, authorization in the context of the web as an open space) was that the code-based approach and the contract-based approach were inadequate in that the former exempts from the scope any access that code allows and also includes under the scope any access that is only mildly frustrated by code (it over- and under-includes, respectively), and the latter fails because of the breathtaking, rather alarming, notice issues and serious risk of arbitrary enforcement that accompany it. The agency-based approach,

[1065] *LVRC v. Brekka*, 581 F.3d 1127, 1136 (2009)
[1066] See also an analysis of *Brekka* and the court's use of the rule of lenity in Warren Thomas: Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act (2010), Georgia State University Law Review, Volume 27, Issue 2, Article 14. Available at http://readingroom.law.gsu.edu/gsulr/vol27/iss2/14.

which is only applicable in situations where an agency relationship exists, leaves no possibility of giving "exceeding authorized access" any meaning, since access for a purpose contrary to the interest of the employer automatically de-authorizes the employee completely, leading to only "without authorization" being applicable in insider cases, even though it is clear that Congress intended "exceeding authorized access" to apply to insiders.

Kerr suggests a social norms approach that is rooted in the trespass doctrine, as mentioned before, and proposes a three-pronged analysis to determine authorization based on traditional common law trespass analysis; (1) the nature of the space, (2) the means of access, and (3) the context of entry. Whereas, the chapter on outsiders mainly discussed open spaces (i.e. spaces where the information is accessible to anyone, and thus, no one is truly an insider), this chapter, discusses closed spaces that require special permission to access.

For example, the nature of the space in *Brekka* is closed. LVRC specifically delegated special access authorization to Brekka – authorization that LVRC would only delegate to an employee, not just any random person who requests access authorization. The documents obtained by Brekka resided within a security perimeter that required Brekka to authenticate himself at the perimeter. Brekka had been given access credentials so that he could authenticate himself as a person authorized to access the documents. Those access credentials were a result of delegation of authorization to Brekka. Thus, there was nothing abnormal about how Brekka gained access, because he used a password where a password was required, and furthermore, there was a clear line of delegation of authority from the computer owner to Brekka. He did not use another person's password or guessed a password in order to masquerade as a legitimate user. A closed space indicates that special authorization is required in order to gain legal access. Brekka had that authorization because, as an employee of LVRC, he was granted such authorization. After the employment ended, the space would of course remain closed, and even if LVRC had failed to deactivate Brekka's access credentials (means of access would remain consistent with social norms), Brekka's authorization to access would have been revoked as a result of the employment having ended.

Although the typical idea of an insider is an employee or other person who truly has privileged access to information that is not publicly accessible, in cases such as *Drew* one would be hard pressed not to view Drew as an insider of sorts in some respects, at least regarding access to her own account. But she would not be an insider in all respects or even in the most important respect

that she has access to information that MySpace wants to keep from the public; Drew only had access to information that she herself might want to keep from the public. Drew created a personal account with MySpace and only her access credentials would provide access to the account. Yet, it is hard to imagine that merely having created a social network account would make one an insider with respect to the computer(s) that contains all information pertaining to the account. For example, as a hypothetical scenario, let us imagine that a person has a Facebook account. That person then later goes on to hacking into another person's Facebook account, or even Facebook's employee mail server. One would again be hard pressed to characterize the perpetrator as an insider with respect to Facebook merely by virtue of having registered for a Facebook account or merely because some or all of the information accessed happened to reside on the same hardware.

In the past, it was much easier to determine whether one was exceeding authorized access to a computer by accessing information one was not authorized to access (remember, earlier in the dissertation it was argued that exceeding authorized access meant accessing a computer to which one had authorization to access, and accessing information on that computer that one was not authorized to access). Today, cloud computing makes it hard or impossible not to access multiple computers just when accessing one's own data in the cloud, since data may be spread around across many computers in many jurisdictions (which also begs the question whether a breach of terms of service would then trigger criminal liability in every single jurisdiction where the information and computers may reside). In most cases involving unauthorized remote access to information, physical hardware becomes irrelevant in determining whether access was authorized or not. For example, a webserver could very well be hosted on the same physical hardware that also hosts another system for another system owner. The same hardware can host many virtual machines, but is it the access to the computer as a piece of hardware that counts or is it the access to the computer as an information system that counts? Imagine that one has been banned from accessing a website that is hosted on the same hardware as thirty other websites. Given the language of the CFAA, how could a court qualify one website owner's de-authorizing of another person's access to the website (if one were intent on letting the CFAA cover such situations)? The only way would be to qualify the access to the *computer* (the hardware) as being in excess of authorization, since the hardware hosts 29 other websites that the banned person is still authorized to access, and over which this particular website owner cannot exercise proprietary rights, such as the right to exclude others. But the banned person would almost always be oblivious to the fact that the website is hosted on the same hardware as 29 other websites that he still has authorization to access, unless he for some

reason were interested enough to look up that fact. Does the fact that the website owner happens to use shared hosting really make the banned person an insider with respect to the website from which he now is banned, just because the hardware happens to host other websites that he is still authorized to access? The point is, that in today's world of IT, anyone can be construed as an "insider" because we all have authorization to access an enormous number of computers and yet only have very limited rights to access information on those computers; that information typically being information created by us or otherwise belonging to us, or information that has been made publicly accessible by the computer owner or service provider. But our account information may reside on the same *computer* as account information of thousands or millions of other people.

12.2.5.1 Accounts

Accounts are closed spaces, because they require authentication to access and thus create a barrier with respect to access by others who have not been authorized to access. I.e. accounts are a specific delegation of authorization to access information or services.[1067] This characteristic of accounts sufficiently distinguishes them from websites that allow free and open access by any member of the public. If the account is blocked, then authorization is withdrawn and access becomes unauthorized. This would be true regardless of whether the blocked account is an Instagram account (which any member of the public can create at any time) or an employee account within an organization. However, whereas an employee would be barred from simply creating a new account, an Instagram user can create a new account if his old account is blocked. As Orin Kerr points out, where an account requires no special relationship with the online service and a new account can easily be created, a prior blocking of a user's account does not necessarily mean that he is completely barred from interacting with the service or even create a new account. It depends on the context. For example, the user's actions that led to the blocking of the first account, the user may not intend to repeat with his new account because he risks losing access to his new account.[1068] However, if the

[1067] See Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 31. Available at: http://ssrn.com/abstract=2601707
[1068] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 33. Available at: http://ssrn.com/abstract=2601707

user is informed that he cannot create a new account ever again (a total ban), that might make his access unauthorized.[1069] Such a direct action should at least be required to revoke authorization.[1070]

As pointed out in the above section on former employees, even though an employer fails to block or delete the account of a former employee, the former employee does not retain authorization to access the account merely because it is still active. As was made clear in *Sablan*, if the relationship between the employer and the employee ends, then the authorization to utilize that account is revoked, even if the account still allows access.[1071] That is, access subsequent to the end of employment is unauthorized. The employment relationship provides the context in which access to a closed space becomes authorized, whereas an ended employment relationship means that there no longer is any delegation of authorization as required because of the closed nature of the space.

Thus, the circumventing a total ban where the space is open should not incur criminal liability, because IP blocking, for example, is aimed at an IP address, which the user is free to change and frequently will change without the user getting requesting so, anyway. That is, in open space, those who attempt to block certain users are blocking them based on characteristics that are under the user's control – not the person who is doing the blocking. Conversely, in closed space, the person doing the blocking is in complete control of the access possibility, because he can simply block or delete the account. Circumventing that ban will in some contexts be acceptable, such as where anyone can sign up for an account, e.g. a gmail account, because the blocking of an account does not necessarily preclude the owner of the blocked account to create a new account and then avoid the behavior that caused the first account to be block. This context differs from the context of employee accounts on work computers. Once that account is blocked or deleted that definitively means that the employee is no longer authorized to access the system, and the same applies where the account remains active, but the employee has been terminated or has resigned. Authorization is not automatically revoked when a user violates the terms of use or service; the revocation of

---

[1069] Arguably, the courts should be wary with respect to allowing just any such claim of unauthorized access to pass without scrutinizing the claim; especially, in light of the fact that just about any violation of terms of service might cause the provider to ban the individual, and that some violations may carry with them a permanent ban. Recall that acting against the spirit of Facebook's terms of service constitutes a breach of those terms. The particular concern here would probably primarily be speech, that otherwise is not criminalized and thus protected, but becomes criminalized by proxy (via the hacking statute), because free speech rights may not be enforceable against a private actor, who claims his services were accessed without authorization subsequent to undesirable speech.

[1070] See Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 34. Available at: http://ssrn.com/abstract=2601707

[1071] Obviously, if there is some sort of agreement regarding continued access, then the authorization is not revoked, even if the employer-employee relationship ceases to exist.

authorization depends on a direct action taken by the owner of the system.[1072] Such an approach would also conform better to the fact that breaches of contract do not automatically discharge the contract, but requires the party to rely on a particular remedy available to him, one of which may involve the discharge of the contract.

12.3 Insiders in Danish law

In 1986, the late Professor Vagn Greve addressed computer crime in a short book called "edb-strafferet" (computer crime law).[1073] Due to the very limited number of computer crime cases in Denmark at the time, he also looked to the US and to the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (the precursor to the CFAA), as well as some computer crime related prosecutions under the US mail and wire fraud acts.

He also briefly addressed insiders with respect to their access to and use of computers and information on them. Greve argued that unauthorized use of the employer's computers for purposes unrelated to the employee's job was not necessarily criminal under § 293(1), which prohibits the unauthorized use of things belonging to others. He argued that for the criminal law to apply, the misuse must reach a certain level of seriousness; the misuse could not be of a trivial character, such as playing a computer game during a break or writing personal Christmas cards.[1074] If the misuse were excessive in nature, remedies available in civil law should apply, rather than letting such misuse trigger criminal liability.[1075] However, if the misuse for example involves using the employer's computer to build up a competing business, such misuse would trigger the application of § 293(1).[1076] Thus, Greve seemed to focus on the purpose of the misuse; his argument seems also to implicate use for purposes that are disloyal to the employer. However, a 1996 case, which is analyzed below, indicates that purpose may not matter.[1077]

As noted previously, the legislative history of the Danish hacking provision also distinguishes between insiders and outsiders, even though the same statutory language covers both. Trade secret

[1072] Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 34. Available at: http://ssrn.com/abstract=2601707
[1073] Vagn Greve: edb-strafferet (1986)
[1074] Vagn Greve: edb-strafferet (1986), p. 22
[1075] Vagn Greve: edb-strafferet (1986), p. 22
[1076] Vagn Greve: edb-strafferet (1986), p. 23
[1077] Of course, a single High Court decision is not sufficient to state with certainty that all the courts will now ignore the purpose of the access. It remains to be seen whether the 1996 case is the correct interpretation of § 263(2) and (3).

law also applies with respect to employees who improperly obtain trade secrets and employees who use or share trade secrets without being authorized to do so. I.e. there is some overlap between trade secret law and the criminal code's § 263(2) and (3), because the Marketing Act § 19 also covers unauthorized obtaining of a specific type of information: trade secrets. The Marketing Act § 19 covers much more than mere unauthorized access to (obtaining of) trade secrets. It also prohibits unauthorized use and disclosure of trade secrets. Thus, whereas the criminal code § 263(2) and (3) prohibit unauthorized access to trade secrets, the Marketing Act § 19, additionally covers situations where the access to the trade secrets was authorized, but the trade secrets were misappropriated, i.e. disclosed, used, etc. That is, the scope of the Marketing Act § 19 goes beyond mere access and also addresses what happens subsequent to the access, regardless of whether the access itself was authorized or unauthorized.

The trespass provision in the criminal code, § 264(2), like § 263(3), states that criminal trespass that is committed with the intent to obtain trade secrets is subject to a harsher penalty bracket than simple trespass absent any aggravating circumstances. That is, in cases involving access to trade secrets, it is an indispensable prerequisite for a finding that there has been a violation of § 264(2) and § 263(3) that the access has already been found to be unauthorized under § 264(1) and § 263(2), respectively. The fact that trade secrets were accessed is not sufficient to trigger criminal liability; the access must also be unauthorized. Accessing trade secrets is only an example of purpose of access. Purpose of access may trigger an enhanced penalty bracket, but purpose of access does not determine whether the access was authorized. This is illustrated in U 1996.979Ø.

In U 1996.979Ø, an employee in a bank had accessed trade secrets on the bank's computer system, using his own password, and printed out confidential information, shortly before resigning from his position. The employee was initially found guilty of unauthorized access (§ 263(2) and (3)) in the district court but was acquitted on appeal. It appears to have been the prosecution's theory that the access was unauthorized because the employee did not access the information for any business-related purpose.[1078] The prosecution also alleged that the defendant must have known that his authorization would be rescinded the moment he tendered his resignation.[1079] The district court found the defendant guilty arguing that the defendant's access trade secrets shortly prior to his

[1078] U 1996.979Ø, p. 980
[1079] U 1996.979Ø, p. 980

resignation was unauthorized regardless of the fact that he used his own password.[1080] On appeal, the High Court disagreed and acquitted the defendant. The High Court held, briefly (as is customary in Danish court decisions), that the defendant, being an employee at the time of the access, had access to the bank's computer system, and thus, it was not unauthorized access when the defendant did so using his own password. Furthermore, the High Court added that it was not proven that the defendant had known that his authorization to access the system would have been rescinded immediately upon tendering his resignation. The High Court's concise opinion steers perfectly clear of any mention of purpose for the access. The defendant was an employee at the time and had authorization access to the system and the information in question; ergo, his access was authorized.

The prosecution clearly invited the High Court to indulge in a construction of "authorization" that would entail an examination of a defendant's purpose for accessing information, but the High Court's silence on the matter equally clearly calls for the inference that purpose for access cannot negate the existence of authorization.[1081] However, it is unclear what role, if any, it would have played had the defendant been found to have been aware that his authorization would be rescinded later the same day. There were no allegations of access after the authorization had in fact been withdrawn when the employee resigned. Anticipation of the rescinding of authorization in the immediate future would not render the defendant's access any more or less non-business-related compared to if he had not anticipated the revocation of authorization. Nor can an anticipated revocation be equate with an actual, affirmative, instant revocation of authorization; otherwise, the mere anticipation of revocation would in itself automatically implicitly revoke authorization to access even prior to the employee's resignation and without any affirmative steps taken by the employer to actually revoke authorization.

Make no mistake, the fact that the password works and thus technically allows access is not important. In *United States v. Sablan* the defendant had used her still-active password after her employment ended. The defendant in the Danish case was still employed at the time of access. Sablan's authorization was revoked when her employment ended, but the Danish defendant's employment had not ended at the time of access, even though he intended to resign later that day. The fact that the password grants access does not mean the access is authorized; as is apparent from

[1080] U 1996.979Ø, p. 980

[1081] Mads Bryde Andersen opines that the High Court decision must be erroneous in Mads Bryde Andersen: IT-retten (2005), p. 746. I disagree.

cases where a person guesses or steals another person's password. The important question is whether authorization had been delegated by the owner to the person using the password. In the Danish case, the answer is yes. Under circumstances such as those in *Sablan*, the answer would be no, because the employment had already ended at the time of access, and thus, there was no authorization delegated to the defendant at the time of access.[1082] From that perspective, the prosecution in the Danish case was part right and part wrong; the fact that the defendant had used his own password, and the fact that it worked, was immaterial to authorization as such, but the defendant's authorization to use that password flowed from his status as employee at the time of the access regardless of what he may or may not have intended to do in the future. The access would have been undesired regardless of whether the employee had intended to resign later that day, in a month or not at all. Arguably, it would have been much more fruitful for the prosecution to prosecute the defendant for attempted violation of trade secret laws (the misappropriation, intent to disclose or use or the likes) rather than trying to get the defendant convicted for a completed crime of unauthorized access on a theory that the access was unauthorized because the defendant had allegedly misappropriated confidential information the day he resigned.

The prosecution's theory shows the serious weakness of any construction of "authorization" that implicates the purpose of access. It would be no different than prosecuting a person for trespassing in a supermarket because the hypothetical defendant entered to buy anti-freeze they intended to use to poison someone. Of course, the supermarket, had they known the hypothetical defendant's purpose, would never have allowed him access. The unwanted behavior is not the access to the store nor the purchase of anti-freeze, but the attempted murder. If purpose is invoked to negate already existing authorization, any regular activity can be made criminal as long as the access is a step in preparation of the illegal conduct the defendant intends to engage in later.[1083] Of course, the nature of space in this example is different from the nature of the space in the Danish case, but the point is simply that an objectionable purpose for legal conduct can be rendered illegal if the purpose of legal conduct is allowed to negate its legality. It is arbitrary, and generally has not place in open nor closed spaces.

[1082] See also Orin S. Kerr: Norms of Computer Trespass (May 2015 draft) Columbia Law Review (Forthcoming 2016), p. 32. Available at: http://ssrn.com/abstract=2601707
[1083] See e.g. *United States v. John* discussed above.

Furthermore, enquiring as to purpose could render any violation of data protection laws an automatic violation of the hacking provision even though violation of data protection law is already separately criminalized in the Data Protection Act. Conflating purpose of use or purpose of access with access authorization significantly inflates that the scope of an illegal access provision. Contrary to a general illegal access provision, the data protection law actually focuses on purposes of processing personal information, rather than merely access to information. For example, if a data controller or processor processes information for purposes contrary to law or contract, the information was inevitably accessed in the process, and thus accessed for an illegal or unwanted purpose.[1084] Ergo, implicating purpose of access (i.e. intended use of information accessed) converts data protection law violations into criminal hacking, subject to imprisonment up to six years instead of the maximum of four months under data protection law.[1085]

In another Danish case, U 2004.2204Ø, the defendant had obtained and disclosed, for non-business reasons, credit information from a credit information database he had access to by virtue of his employment at a real estate agency. He was prosecuted for violating the Data Protection Act because he had no legal purpose for obtaining the personal information as required under data protection law. He was not prosecuted for unauthorized access under the criminal code's § 263(2), and arguably, such a prosecution would have been less than fruitful because the defendant clearly had authorized access to the database, regardless of whether his later use of the information he obtained was illegal under other laws.

12.4 Summary

As mentioned in the chapter explaining the structure of the dissertation, the Convention and EU law were omitted from the chapter on insiders, because the Convention and EU cybercrime law does not offer anything new with respect to insiders that does not equally apply to outsiders. Thus, covering the Convention and EU cybercrime law again in this chapter would be quite redundant. There is a single important exception with respect to EU law. The Directive on attacks against information systems exempts labor disputes and terms of service/use from its scope. Thus, every EU country,

[1084] See generally Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[1085] See the Danish Data Protection Act § 70.

except Denmark, will be barred from enforcing their domestic implementation of the illegal access article in cases where the only basis for lack of authorization is a breach of terms or a labor dispute. This may have been done for a good reason, which could also be used (although, unlikely to succeed) with respect to the CFAA and agency and contract-based approaches to the interpretation of authorization. Namely, a combination of the principle of subsidiarity and the fact that competences which have not been conferred upon the Union are retained by the member states, who can freely legislate in those areas retained. The Tenth Amendment to the United States Constitution[1086] similarly states the United States can only act within the boundaries of the competences conferred upon it. A claim based on the Tenth Amendment is highly unlikely to succeed and the US Supreme Court has stated that the Amendment merely states a truism.[1087] Considering that the CFAA was adopted on the basis of the commerce clause, which is exceptionally broad as a legal basis, it is unlikely that a Tenth Amendment challenge against the CFAA would succeed. Conversely, the Directive was adopted on the basis of a treaty article that is limited to criminal law cooperation, not the treaty article that closely resembles the broad commerce clause of the United States Constitution, the Directive arguably cannot, on that legal basis, encroach on member states' national law so as to displace domestic trade secret laws and contract law.

Also a likely explanation is that a trade secrets directive that addresses the illegal obtaining, disclosure and use of trade secrets has already been proposed.[1088] That is, the specific harm is being more appropriately addressed in its own directive rather than relying on convoluted and very broad constructions of hacking laws as a proxy to reach undesirable behavior; behavior that in fact occurs subsequent to the access because the offenders often have authorized access to the information, but misappropriate the information.

As explained in the beginning of this chapter on insiders, the concepts of insider and outsider are relative to each other with respect to a given resource. The distinction between without authorization and exceeding authorization is important in the CFAA, because the CFAA focuses on access to the computer. Had the CFAA only forbidden access without authorization, then the statute would only apply where the person accessing had no authorization at all (i.e. is without

[1086] Amendment X: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people."
[1087] CRS Annotated Constitution: Tenth Amendment. Available at Cornell's website at https://www.law.cornell.edu/anncon/html/amdt10_user.html#amdt10_hd7. Last visited on 31 August 2015.
[1088] COM(2013) 813 final. Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

authorization). The only way to get that hypothetical version of the CFAA to cover access to information that the person is not allowed to access would be to ask why he accessed the information and finding him to have accessed without authorization if he had an undesirable purpose for accessing the computer. But adding the language such as "exceeds authorized access" allows application to those who are not without authorization to access the computer, but who nonetheless were not authorized to access the particular information he accessed. Adding the language obviates the need to construe the hypothetical CFAA, which only covers access to the computer that is without authorization, as if it did contain the words "exceeds authorized access".

For example: A is authorized to access a computer to which B lacks any authorization to access. B is then an outsider with respect to A in terms of the computer in question. If B accessed the computer regardless of his lack of authorization, he would be accessing the computer without authorization.

Another example: A is a manager and has authorized access to the HR records relating to his department's employees. Furthermore, he is granted access to case files for cases that are being handled by his department as needed, and is blocked from accessing other cases. B is one of A's employees and is granted access to case files for cases that he is assigned, and access to other case files are blocked. Both B and A are insiders with respect to non-employees and employees of other departments, and B is also an insider with respect to other employees in the department who are not working the same case as he. B is an outsider, and A is an insider with respect to B, in terms of the HR records on the employees in the department. B is also an outsider, and A is an insider with respect to B, in terms of the case files on cases that are being handled by other employees in the department, but are not being handled by B. So, for example, if A accesses HR records on other employees than those in his department he *exceeds* his authorized access. He does not access the computer on which the HR records reside without authorization, because he is allowed to access the computer to obtain files on his own employees. The same applies if B accesses case files related to cases that he has not been assigned. He is authorized to access the computer on which the files reside, so he is not without authorization in terms of access to the computers, but he does exceed his authorized access in terms of the computer because he accessed information on the computer that he was not authorized to access. Purpose of access does not, and should not, matter in any of these examples.

Asking about the *purpose* of access that is otherwise authorized allows the courts to take one step into the future.[1089] For example, if the hypothetical CFAA only prohibits access *without authorization*, asking about purpose of access allows the courts to find a violation as if the statutory

[1089] Marco Gercke makes the same important point in his report written for the United Nations special agency ITU (International Telecommunication Union). See Marco Gercke: Understanding cybercrime: Phenomena, challenges and legal response (2012), p. 178 ("It is vital to distinguish between illegal access and subsequent offences (such as data espionage), since legal provisions have a different focus of protection"), and p. 182 ("In cases where the offender has legitimate access to a computer system (e.g. because he/she is ordered to repair it) and on this occasion (in violation of the limited legitimation) copies files from the system, the act is in general not covered by the provisions criminalizing illegal access.")(citations omitted)(discussing the limitations of coverage of data espionage under the Convention)

language had included *exceeds authorized access*. The courts are essentially asking "well, you have authorized access to the computer, but what happens next?" If the courts ask about purpose when applying the actual CFAA, which contains both *without authorization* and *exceeds authorized access*, then asking about purpose again pushes the scope one step further when the courts again ask "well, you have authorization to access both the computer and the information, but what happens next"? This enables the court to construe the CFAA as if it included prohibitions as to how the information were used after they had been accessed with authorization. Asking about purpose always equates to asking "then what happened?", which is quite problematic where what happened next (i.e. the use of information) is not actually an element of the crime.

Because the Danish criminal code § 263(2) does not prohibit access to computers, but instead prohibits access to information and programs, having both "without authorization" and "exceeds authorization" as a part of the statutory language is not necessary. The Danish criminal code § 263(2) only prohibits access to information and programs "without authorization". Thus, there is no need to construe authorization based on the purpose of the access to a computer. A person who has no authorization to access the computer, also has no authorization to access any information on the computer. If the person accesses information without authorization on a computer to which he has some authorization to access, he also accesses without authorization within the meaning of § 263(2) because the provision targets authorization with respect to the information accessed. Adding "exceeds authorization" to the language of § 263(2) would mean the courts would have to ask about the purpose of accessing information, because the only way authorization to access a piece of information would be to do something more than merely access it. In that case, asking "then what happened?" would be mandated by the language, because the language then obviously asks what happened after the access. But § 263(2) does not contain such language, and thus, asking about the purpose of the access (i.e. what happened after the access) in order to convert an authorized access to an unauthorized access would be contrary to the statutory language, because it would essentially entail adding elements to crime that are not there.

Even though terms of use and service, computer use policies and the likes, state for which purposes information may be accessed, violations of such terms and policies may well constitute a contractual breach, but the contractual breach does not automatically trigger criminal liability, because a contractual breach does not automatically discharge the contract, e.g. employment contract, that provides the authorization. Even if such policies were scrutinized ostensibly solely to establish the scope of the authorization, and the policies stated that information or computers may

only be accessed for certain purposes, the statutory language does not support an inquiry into purposes of access, because resorting to an inquiry into purpose with a view to construing authorization to access, both under the CFAA and the Danish hacking provision, effectively pushes the scope a step further to cover use of information, because access to both computers and information are fully covered under both the CFAA and the Danish hacking provision. Asking why information was accessed is always in inquiry into what would happen after the access, and thus, always adds elements to illegal access statutes such as the CFAA and the Danish hacking provision, as well as provisions that implement article 2 of the Framework Decision, article 3 of the Directive and article 2 of the Convention on Cybercrime. None of these prohibit unauthorized use of information.

A pure code-based approach does not account for all the conduct that one might consider unauthorized access. For example, where a sales employee has discovered he has access to payroll files, e.g. where the system mistakenly allows access, and he obtains information he knows he has not been granted access to; or where an employee uses a non-password protected computer and obtains information. It is important to remember that computers do not consent to anything, but where the nature of the space is open, there is a very strong presumption for authorization that the means and context of the access may negate. Where the nature of the space is closed, access is presumably unauthorized unless it is in the context where the person has been granted permission to access; such as where an employee is granted access because he is an employee. Anyone who has not been granted special permission to the closed space would access it without authorization. A pure and broad code-based approach could also unnecessarily include e.g. circumvention of Facebook blocks on the organization's network, even though such conduct is hardly the type of harm hacking statutes seek to prevent, and it could include those employees who have found a short-cut in the system that allows them to avoid dealing with security protocols, because it is simply a more efficient way to work, but is without any harmful intent; a broad code-based reading could interpret that as a circumvention of a code barrier, even if the employees did so with the organization's best interests at heart. I.e. a lax security culture could mean that access restrictions are not enforced in practice and the restrictions could come back to haunt equally those who

violated them to simply get work done, and those who violated them to harm the organization. This example also shows the thin line between code and contract.[1090] ()

The contract-based approach is for many reasons an inappropriate way of construing "authorization". As mentioned earlier, violation of terms and policies do not automatically discharge the employment contract. It generally requires the employer to act on the breach by using one or more of the remedies provided in contract law. It is particularly odd if a breach of contract can automatically incur criminal liability, but cannot civilly discharge the contract which delegates the authorization. In other words, civilly, the authorization remains despite the breach of contract because the contract has not been avoided, but criminally the authorization is revoked based on the breach of contract. Furthermore, a contract-based approach under which every violation of terms and policies to revoke authorization automatically and incur criminal liability leaves the definition of the crime of unauthorized access in the hands of computer owners who can write whatever they want in their terms and policies. Even if only some breaches automatically revoke authorization and incur criminal liability, the question arises which ones would and which ones would not? It becomes unforeseeable which breaches (and thus which conduct) triggers criminal liability.

As with authorization with respect to outsiders, the social norms-based approach seems the most appropriate. The closed space within which insiders operate typically means that they are authorized to access sensitive information. An approach that at least rejects contract and agency-based approaches, would arguably incentivize organizations to not only secure their outer security perimeter, but classify information by sensitivity and, by code, restrict employees' access to information that they do not need access to in order to do their job. However, because the social norms-approach considers means of access, it is possible that the approach could construe authorization, or lack thereof, to cover acts that are technically a circumvention of a code restriction, such as where a security measure can be trivially circumvented, but the circumvention does not result in access to information the person is unauthorized to access. That is, e.g. if employees start sharing passwords, or perhaps decide to use one password instead of logging another user out and logging themselves in every time they need to service a customer, the means of access is technically not in conformity with general social norms. However, the context norms

[1090] Note that e.g. (a)(2)(C), in cases where the plaintiff or prosecutor opts for pursuing a defendant for access without authorization there is no additional language, such as in the definition of exceeds authorized access, that requires that the information obtained was information the person was not entitled to obtain. The elements of the crime are then only that 1) the access was without authorization and 2) information was obtained.

should be able to adjust for this, by taking into consideration that there had been a delegation of authorization to everyone who used the password that technically did not belong to them, even though such conduct is not optimal from a security point of view.[1091]

Regulating insiders is decisively harder than regulating outsiders, and there is plenty of literature discussing the insider threat. One of the reasons it is so hard to regulate insiders with hacking statutes is that insiders have been granted authorization to access information to which others do not have access. To maximize their protection under unauthorized access statutes, organizations should classify information according to sensitivity and place code restrictions accordingly, allowing employees only to access what they need in order to do their job. Granting carte blanche authorizations to employees in hopes of being able to state a plausible "unauthorized access" claim by referencing written policies and by scrutinizing the purpose of access is not advisable. Where the user has authorization to access, illegal access statutes cannot cover the user's conduct.[1092] The repercussions of giving a statute, which covers both insiders and outsiders, that kind of extensive and vague reach are lack of foreseeability and arbitrariness, as well as, arguably being contrary to the statutory language.

Even though unauthorized access statutes should not be applied in cases where a legitimate user misappropriates trade secrets or other information that is not to say that there should be no law that punishes that conduct. Such laws do exist, and they are a more appropriate way of addressing the harm, which is not the legitimate user's authorized access, but his subsequent unauthorized use of the information. Copyright law, trade secret law and data protection law are just some examples of the legislature's proven ability to legislate against unauthorized use of information regardless of whether access to them was legitimate or not.

[1091] This example was inspired by one of the author's former workplaces, where a password belonging to a former employee was routinely used on a shared computer, because no one could be bothered to keep logging themselves in and out of the system when they had to regularly return to the computer. Every employee who used the improper means of access had been delegated authorization, and the information obtainable was the same for everyone.

[1092] See also Marco Gercke: Understanding Cybercrime: Phenomena, Challenges and Legal Response (2012), p. 182. Available at http://www.itu.int/INT-D/cyb/cybersecurity/legislation.html. Gercke states that authorized users are generally not covered by illegal access provisions.

13 PUBLISHED ARTICLE: AN ANALYSIS OF THE DANISH CRIMINAL CODE § 193 (IN DANISH)

En analyse af straffelovens § 193

(Published in Juristen, Issue 3, July 2015)

Af Helena Lybæk Guðmundsdóttir, ph.d.-stipendiat, International Economic Crime and Cybercrime Research Centre, Juridisk Institut, Aalborg Universitet

Artiklen omhandler anvendelsesområdet for straffelovens § 193, der kriminaliserer den retsstridige fremkaldelse af omfattende forstyrrelse i driften af samfundsvigtige anlæg. Artiklen fokuserer på den usikkerhed vedrørende bestemmelsens anvendelsesområde, som indføjelsen af begrebet "informationssystemer" medførte. Det er forfatterens opfattelse, at bestemmelsen bør fortolkes i lyset af de interesser, som er beskrevet i forarbejderne fra 1917 og 1923, idet man herved dels opnår en acceptabel klarhed over, hvilke typer af informationssystemer, der kan være omfattet, dels undgår en betænkelig og unødvendig udvidelse af bestemmelsens anvendelsesområde. De to store hackersager, der indtil nu har involveret straffelovens § 193, og som er omtalt i denne artikel, viser en problematisk tilgang til og usikkerhed vedrørende fortolkningen af bestemmelsen.

13.1 Indledning

Angreb på centrale informationssystemer gennem hacking er et samfundsmæssigt stort og stadigt stigende problem. I takt med at sådanne angreb opdages og afdækkes, opstår der samtidig et pres på det strafferetlige system for at kunne håndtere sagerne. Straffeloven har ad to omgange været justeret for at kunne anvendes også på cyberkriminalitet, men med vekslende held. Nogle bestemmelser er således helt nye (f.eks. § 279 a), andre er uændrede, men søges ved, en nogle gange anstrengt, fortolkning anvendt på informationsteknologien (f.eks. § 291), og atter andre er i gerningsbeskrivelsen blevet suppleret med en henvisning til informationsteknologien. Dette sidste er tilfældet med § 193. I det følgende beskrives de problemer et sådant miks mellem gamle

bestemmelser med en given beskyttelsesinteresse og nye fænomener, der er søgt dækket med en bred – og måske for bred – henvisning i gerningsbeskrivelsen, kan medføre. Der er endnu ikke meget retspraksis vedrørende § 193 og informationsteknologien, men den praksis, der er, afslører stor usikkerhed hos retsanvenderne. Denne artikel har til formål at mindske denne usikkerhed i kommende sager.

Det er ikke ualmindeligt, at lovgiver anvender brede begreber i lovgivningen, heller ikke i straffelovgivningen. Straffelovens § 193 angik frem til 1985 anlæg med specifikke funktioner af samfundsmæssig betydning. I 1985 vedtog lovgiver beskyttelse af databehandlingsanlæg hvis funktion ikke er specifikt afgrænset. I 2004 valgte man at erstatte begrebet databehandlingsanlæg med det mere teknisk neutrale begreb informationssystemer. Dette medfører, eksempelvis, at alt hvad der kan kaldes informationssystemer falder inden for ordlyden af § 193. Jo mere udbredte informationssystemer bliver og jo flere der kommer, jo bredere bliver bestemmelsen uagtet den reelle vigtighed af de diverse systemer. Bestemmelsens ordlyd skelner ikke mellem, på den ene side, nedbrud af centrale betalingssystemer, NemID, elforsyningen eller trafikdata til lufthavnene, og på den anden side, nedbrud af online spilleplatforme, sociale medier osv. Dette trods den store forskel i vigtigheden af systemerne.

Domstolene stilles derfor over for en vanskelig opgave. Artiklen klargør, at bestemmelsen ikke alene eller overvejende, kan, eller bør, hvile på det, "der kan tælles". Hermed menes den kvantitative størrelse af den berørte personkreds. Forstyrrelser i driften af informationssystemer, der ikke er samfundsvigtige og derfor ikke omfattet af § 193, vil oftest være omfattet af andre bestemmelser i straffeloven, eksempelvis §§ 263, 291 eller 293. Derfor er der ikke behov for at udvide anvendelsesområdet for § 193. En analyse af beskyttelsesinteressen i § 193 er derfor vigtig for at sikre, at bestemmelsen kun anvendes, hvor de beskyttede interesser krænkes.

13.2 Bestemmelsens ordlyd

Ved straffelovens § 193, stk. 1, kriminaliseres den retsstridige handling, der fremkalder omfattende forstyrrelse i driften af almindelige samfærdselsmidler, offentlig postbesørgelse, telegraf- eller telefonanlæg, radio- eller fjernsynsanlæg, informationssystemer eller anlæg, der tjener til almindelig forsyning med vand, gas, elektrisk strøm eller varme.

Bestemmelsen har ikke gennemgået store ændringer siden 1930, da den borgerlige straffelov af 1930 erstattede straffeloven af 1866. I 1985 vedtog Folketinget adskillige ændringer og tilføjelser til straffeloven på baggrund af Straffelovrådets betænkning[1093] om datakriminalitet. En af disse ændringer vedrørte straffelovens § 193. I opregningen af anlæg, der beskyttes efter § 193, tilføjedes bl.a. "databehandlingsanlæg". Straffelovrådet overvejede i 1985-betænkningen at begrænse kredsen af de databehandlingsanlæg, der beskyttes efter § 193, men antog i stedet, at kravet om, at driftsforstyrrelsen skulle være "omfattende", var tilstrækkeligt til at begrænse bestemmelsens anvendelsesområde.[1094]

Man kan af ordlyden udlede fire kumulative betingelser for bestemmelsens anvendelse. Den første betingelse er, at systemet/anlægget objektivt skal være omfattet af bestemmelsen, dvs. skal være en af de typer systemer/anlæg, der nævnes i bestemmelsen. Den første betingelse behandles i afsnit [13.3]. Den anden betingelse er, at der skal være sket en forstyrrelse. Den tredje betingelse er, at den fremkaldte forstyrrelse skal være omfattende. Den anden og tredje betingelse behandles i afsnit [13.4]. Den fjerde betingelse er, at forstyrrelsen skal være retsstridigt fremkaldt. Betydningen af begrebet retsstridighed diskuteres ikke nærmere i denne artikel.

Men er alle informationssystemer lige stillet? Kan alene brugerantallet sige noget om hvor uundværligt og samfundsvigtigt systemet er?

13.3 Anlæg objektivt omfattet af straffelovens § 193

Da den nuværende formulering af § 193 har været relativt uændret siden dens debut i den borgerlige straffelov af 1930, er forarbejderne til denne lov fortsat relevante. Ingen af de senere ændringer har således lagt luft til, suppleret eller på anden måde lagt op til en ændret fortolkning heraf.

13.3.1 Generelt om de beskyttede anlæg

Der blev produceret tre betænkninger i forbindelse med forberedelsen af den borgerlige straffelov af 1930. Kommissionsbetænkningen af 1912 forklarer, at grunden til, at den foreslåede § 394 (nuværende § 193) er placeret i kapitlet om andre almenskadelige handlinger er, at det er

[1093] KBET nr. 1032/1985
[1094] KBET nr. 1032/1985 s. 42. Se også gentaget i KBET nr. 1417/2002 s. 139.

"Almenheden, nemlig Publikum i Almindelighed som interesseret i de Paragraferne ommeldte Indretningers uforstyrrede Funktioneren, der angribes ved Handlingerne."[1095] Yderligere forklares i betænkningen, at der er tale om retsstridige angreb på almene samfærdselsmidler og indretninger, der opfylder basale behov, der satte disse offentlige eller offentlig godkendte indretninger ud af brug. Uden for anvendelsesområdet vil kun falde private anlæg med en meget begrænset brugerkreds, og som ikke engang har en indirekte interesse for almenheden.[1096]

I Carl Torps betænkning af 1917 kritiseres bestemmelsen for de meget almindelige og omfattende begreber, der dannede grænsen for bestemmelsens anvendelsesområde, navnlig fordi det i 1912 definerede anvendelsesområde ville inkludere, for eksempel, apoteker, trykkerier (hvis man valgte at anse f.eks. aviser som en almen fornødenhed), fødemiddelforretninger når der krævedes bevilling for driften, osv.[1097] Det fandtes derfor vigtigt at begrænse anvendelsesområdet til virksomheder, der allerede var særligt beskyttede i lovgivningen. Begrænsningen udgør i princippet dele af den, vi kender fra den nugældende § 193, nemlig 1) jernbaner og lignende transportmidler, 2) telegraf- og telefontjenesten, og 3) anlæg, der tjener til almindelig forsyning med vand, gas eller elektrisk strøm. Dertil konkluderede man, at *"[d]erigennem værnes utvivlsomt de vigtigste af de Indretninger, som under de bestaaende Samfundsforhold opfattes som uundværlige."*[1098]

I kommissionsbetænkningen fra 1923 uddybes det, at kapitlet om andre almenskadelige handlinger, omfatter handlinger, der ikke i sig selv er almenfarlige, men som rammer almeninteresser. Nærmere forklares specifikt i forhold til den foreslåede § 177 (forslag til nuværende § 193), at der er tale om almenskadelige handlinger, *"fordi Borgerne i Almindelighed er interesserede i, at Driften af de der omtalte Anlæg og Indretninger ikke forstyrres."*[1099] Kommissionen er enig i betænkelighederne ved, at give bestemmelsen så bredt et anvendelsesområde, som foreslået i 1912. I denne forbindelse diskuterer man særligt betænkelighederne ved en mulig anvendelse af reglen på ulovlige arbejdsstandsninger. Kun når disse arbejdsstandsninger *"direkte rammer de Indretninger, som under den bestaaende Samfundsorden er uundværlige for Borgerne, saaledes at der fremkaldes en omfattende Forstyrrelse i Driften af disse Indretninger, maa Samfundet kunne søge Beskyttelse ved Anvendelse af Straf."* Herefter foreslår Kommissionen bestemmelsen begrænset til, i princippet, de

[1095] Straffelovkommissionens betænkning af 1912, mot. 323
[1096] Straffelovkommissionens betænkning af 1912, mot. 323
[1097] Carl Torps betænkning af 1917, mot. 168
[1098] Carl Torps betænkning af 1917, mot. 168-169
[1099] Kommissionsbetænkningen af 1923, mot. 295

samme anlægstyper, som foreslået af Carl Torp i 1917, og som vi kender fra den nuværende § 193, nemlig: 1) almindelige samfærdselsmidler, 2) offentlig postbesørgelse og almindeligt benyttede[1100] telegraf- og telefonanlæg, og 3) anlæg, der tjener til almindelig forsyning med vand, gas og elektrisk strøm. I umiddelbar forlængelse af afgrænsningen af de beskyttede anlæg fremhæver Kommissionen, at ikke enhver forstyrrelse i driften af disse indretninger er strafbar. Strafbarheden er betinget af, at forstyrrelsen er omfattende. *"Kun derved antager Handlingen en almenskadelig Karakter."*[1101]

Gennemgående i alle betænkningerne er hensynet til *almenhedens interesse*, og at de beskyttede indretninger er *særlig vigtige og uundværlige* for borgerne. Yderligere begrænsede man de beskyttede anlæg til anlæg, der var særligt beskyttede under den gældende lovgivning. Man afviste eksplicit den i 1912 oprindelige foreslåede bestemmelses afgrænsning, hvor begrænsningen af anvendelsesområdet lå i, at indretningerne var offentlige eller offentlig godkendte, og at de tjente opfyldelsen af almenhedens basale behov. Det er derfor klart, at indretninger, blot fordi de er offentlige (eller offentlig godkendte), ikke alene af den grund er beskyttede af § 193.

Derudover, som yderligere baggrund for begrænsningen af beskyttelsen til de opregnede anlæg, beskytter bestemmelsen kun anlæg, der er *uundværlige for borgerne*.

13.3.2 Tilføjelsen af "databehandlingsanlæg"/"informationssystemer"

I 1985 indføjes "databehandlingsanlæg" samt "radio- og fjernsynsanlæg" til de i § 193 beskyttede anlæg. For så vidt angår radio- og fjernsynsanlæg lagde Straffelovrådet vægt på, at disse anlæg sammenholdt med andre anlæg, der omfattes af § 193, har fået en *"stadig stigende samfundsmæssig betydning som kommunikationsmidler"*.

Blot få eksempler af omfattede systemer er nævnt i forarbejderne. For eksempel nævnes den centrale elektroniske databehandling hos de store banker, motorregistret og SKATs centrale systemer. De lokale filialer og skattekontorers terminaler er nævnt som eksempler på ikke-omfattende forstyrrelser, da virkningerne af forstyrrelsen i disse tilfælde ikke vil antage den efter § 193 påkrævede almenskadelige karakter.[1102]

[1100] "almindelige benyttede" blev fjernet fra bestemmelsen i 1985.
[1101] Kommissionsbetænkningen af 1923, mot. 295-296
[1102] LFF 2003-11-05 nr. 55 og KBET nr. 1417/2002, s. 139 (henvisning til Justitsministeriets svar til Folketinget)

Det bemærkes, at alle de i § 193 beskyttede anlæg, bortset fra "databehandlingsanlæg"[1103], har en specifik funktion. Derimod kan databehandlingsanlæg indgå både som angrebsmiddel i forhold til angreb på alle de andre opregnede anlæg, og desuden også indgå som led i driften af hvilken som helst type virksomhed – også dem, man i de tidligere forarbejder fra 1917 og 1923 eksplicit ønskede at udelade fra anvendelsesområdet, og som i øvrigt ikke nødvendigvis, selv under vores nuværende samfundsorden, vil betragtes som *uundværlige for borgerne*. Inklusionen af "databehandlingsanlæg" udvisker, i det moderne IT-baserede samfund, den ellers rimelig klare afgrænsning mellem de *for borgerne uundværlige anlæg* og andre anlæg. Den mere eller mindre indbyggede kvalitative afgrænsning eksisterer ikke i forhold til informationssystemer. Straffelovrådet i 1985 og Brydensholt-udvalget i 2002 overvejede begge, men afstod i sidste ende også begge fra at begrænse kredsen af de beskyttede radio-, fjernsyns- og databehandlingsanlæg, med det rationale, at kravet om, at driftsforstyrrelsen skal være "omfattende", begrænsede bestemmelsens rækkevidde i tilstrækkeligt omfang.[1104]

Straffelovrådets konklusion fra 1985 førte senere til, at Justitsministeriet i sin besvarelse af spørgsmål fra Retsudvalget om, hvad der bør forstås ved "omfattende forstyrrelser i driften", udtalte, at *"[d]e anførte udtryk »omfattende forstyrrelse af driften« og »almenskadelig karakter« angiver, at der må anlægges en kvantitativ vurdering af angrebets omfang. Man må formentlig herved lægge afgørende vægt på størrelsen af den personkreds, der berøres af angrebet."*[1105]

Denne fortolkning blev efterfølgende gentaget i Brydensholt-udvalgets betænkning nr. 1417/2002 om økonomisk kriminalitet og datakriminalitet, samt i 2003 i Justitsministeriets bemærkninger[1106] til det lovforslag som betænkningen førte til.[1107] I forbindelse med fortolkningen af det kvalitativt afgrænsende element henviser man altså blot til det kvantitative afgrænsende element.

Den funktionsbaserede (kvalitative) afgrænsning baseret på, hvilke anlæg, der opfattes som de vigtigste indretninger, der er uundværlige for borgerne under den bestående samfundsorden, forsvinder derfor i vidt omfang ved tilføjelsen af "informationssystemer" i det IT-baserede

[1103] Og måske i mindre grad "radio- og fjernsynsanlæg", da formentlig ikke alle radio- og fjernsynsanlæg vil være lige vigtige.
[1104] Straffelovrådets betænkning nr. 1032/1985, s. 42
[1105] FT 1984/1985 B.1922
[1106] Der står ganske vist "kvalitativ vurdering" i bemærkningerne, men dette må være en stavefejl, da der er tale om henvisning til og betydelig afskrift fra FT 1984/1985 B.1915-1922. Dvs. der er klart tale om opsummering af forarbejderne.
[1107] LFF 2003-11-05 nr. 55

samfund[1108], hvor den eneste tilbageværende afgrænsende faktor er størrelsen af brugerkredsen. Dermed ender man tilsyneladende og uden nærmere overvejelser med en bredere gruppe af beskyttede anlæg, set ud fra de individuelle anlægs funktioner i samfundet. Er angreb på Berlingskes hjemmeside nu beskyttet efter § 193, fordi avisen er tilgængelig i digital form og sandsynligvis har tusindvis af læsere? Pressevirksomhed er jo ellers ikke nævnt som et beskyttet anlæg. Anlæg, der oprindelig ikke var beskyttet, da de i egenskab af deres primære funktion ikke er blevet medtaget i opregningen af beskyttede anlæg, vil nu kunne beskyttes, hvis informationssystemet indgår som led i deres distribution til brugerne, alene i lyset af brugerantallet. Uden den kvalitative vurdering af det pågældende informationssystem vil bestemmelsens anvendelsesområde være på linje med den kritiserede foreslåede bestemmelse fra 1912, der i det mindste, på den kvalitative side, begrænsede anlægstyperne til offentlige eller offentlig godkendte indretninger. Den kvalitative afgrænsning af bestemmelsens anvendelsesområde med "databehandlingsanlæg" [1109], der i 2002 blev erstattet med det mere neutrale "informationssystemer", er dermed forsvundet.[1110]

Afgrænsningsproblemet er ikke nyt. Selvom der er tale om informationssystemer, som ikke fandtes i 1917, så er afgrænsningsproblemerne reelt en gentagelse af historien. I 1917 anerkendte man også, at en nærmere opregning af beskyttede anlæg *"altid maa blive noget vilkaarlig, og at der derfor altid vil kunne rejses Tvivl om, hvorvidt alle de Virksomheder, ved hvilke der er Trang til et saadant Værn, og omvendt kun disse, er medtagne, maa erkendes. Men Ulemperne derved er formentlig væsentlig ringere end Faren ved en Afgrænsning, der holdes i alt for ubestemte og omfattende Udtryk."*[1111]

Domstolene har da også i relation til de oprindeligt omfattede typer af anlæg været opmærksomme på bestemmelsens specifikke beskyttelsesinteresse. I en sag omhandlende en havneblokade[1112],

---

[1108] Man kan, og bør vist også, stille det samme spørgsmål til radio- og fjernsynsanlæg, da det i hvert fald kan diskuteres i hvor høj grad, f.eks. en udsendelse af et afsnit af Hammerslag er "uundværligt for borgerne", sammenholdt med f.eks. nødudsendelser, nyheder, meddelelser fra myndighederne eller lignende. Man kan i hvert fald argumentere for, at der er en kvalitativ vigtig forskel, og man burde stille spørgsmålstegn ved om alle radio- og fjernsynsanlæg, og informationssystemer fortjener en beskyttelse efter § 193 i lyset af bestemmelsens forarbejder.

[1109] Vagn Greve fremhæver også i sin bog EDB-kriminalitet (2. Rev.udg. 1986, s. 23-24), at placeringen af § 193 i kapitlet om andre almenskadelige handlinger indebærer at der skal være tale om særlig vigtige databehandlingsanlæg. *"Bestemmelsen kan næppe bruges, hvis virkningerne alene føles inden for den pågældende virksomhed selv."* (s. 23) Endvidere skriver Greve, at *"[d]et er kun de færreste anlæg, der er beskyttet af § 193, og de fleste forstyrrelser må derfor bedømmes efter andre regler."* (s. 24)

[1110] Brydenholts-udvalgets betænkning nr. 1417/2002, s. 141, jf. s. 71.

[1111] Carl Torps betænkning af 1917, mot. 168

[1112] U 1981.679B

lagde Københavns byret således vægt på, at nogle fiskekuttere havde blokeret for færgeankomster og -afgange i ca. halvanden dag (antageligt som begrundelse for at forstyrrelsen derved havde været omfattende). Retten synes implicit ikke at tage anden havnetrafik end færgetrafik til offentlig transport i betragtning, hvilket også er i overensstemmelse med, at det er almindelige samfærdselsmidler, der er beskyttet. I en anden sag fra 1986[1113], omhandlende en lastbilblokade af et befærdet kryds i udkanten af København i myldretiden, blev de tiltalte frifundet i landsretten. Retten konkluderer, at selvom privatbilismen er et uundværligt led i samfærdslen, findes det betænkeligt, når bestemmelsens ordlyd sammenholdes med forarbejderne, at anse sådan trafik for omfattet af begrebet almindelige samfærdselsmidler. Dette svarer i princippet til den dissentierende byretsdommers opfattelse, nemlig at almindelige samfærdselsmidler kun omfatter transportmidler, offentlige eller private, som offentligheden har adgang til. Dette burde ikke udvides til at omfatte privatbiler. Dvs. et "anlæg" kan være uundværligt, men hvis ikke det er objektivt omfattet af begreberne i bestemmelsen, så er anlægget ikke beskyttet.[1114]

Et tilsvarende problem vedrørende afgrænsningen kender vi fra radio- og fjernsynsanlæg. Det kan også her tænkes, at ikke alle radio- og fjernsynsanlæg pr. automatik er omfattet af bestemmelsen. Der foreligger ingen domme herom, men begrebet fjernsyns- og radioanlæg lider af samme svaghed som begrebet informationssystemer, dog i mere begrænset omfang.[1115]

I en sag omhandlende afbrydelse af udsendelse af tv-avisen[1116] blev der lagt vægt på, at der var tale om et landsdækkende program, der sås af mange mennesker. At fjernsynsanlægget var objektivt omfattet, tog man tilsyneladende for givet, hvilket i den pågældende sag heller ikke uden videre kan kritiseres. Afgørelsen må imidlertid ikke lede til, at enhver afbrydelse af udsendelse af andre kanaler eller programmer, vil være omfattet af § 193. Ligesom ved informationssystemer, fravalgte man som sagt også at afgrænse kredsen af de beskyttede radio- og fjernsynsanlæg nærmere, med samme rationale, nemlig at man må lægge størrelsen af brugerkredsen til grund. Efter forarbejderne til bestemmelsen må der således foretages en kvalitativ vurdering af, hvorvidt en specifik kanal er

[1113] U 1986.423/2 Ø

[1114] Her er tale om, at retten afviser en udvidende fortolkning af begrebet almindelige samfærdselsmidler. Dette er selvfølgelige ikke identisk med at fortolke begrebet informationssystemer indskrænkende. Vigtig er dog at notere, at lovgiver ikke har inkluderet privatbilismen efterfølgende. Dette trods, at retten identificerede privatbilismen som et uundværligt led i samfærdslen.

[1115] Det bemærkes, at DR's monopol på landsdækkende tv-udsendelser først blev ophævet i 1988, hvorfor begrebet "fjernsynsanlæg" i 1985 var begrænset til at omfatte én enkelt landsdækkende kanal, og eventuelt nogle få lokale tv-stationer. Desuden varede DR's monopol på landsdækkende radioudsendelser indtil 2003. Der eksisterede dog en række lokale radiostationer.

[1116] U 2001.1187Ø; der henvises også til denne dom i afsnittet om fortolkningen af begrebet "omfattende".

omfattet af bestemmelsen eller ej. Kanalerne og programmerne vil således langt fra altid have den kvalitative karakter af at være uundværlige og, at "omfattende" forstyrrelse i driften derfor er almenskadelig. På den anden side er det, som nævnt, også klart, at begrebet "fjernsynsanlæg" i sig selv dog er bedre afgrænset end begrebet "informationssystemer", i den forstand, at alle og enhver kan levere en ydelse af en eller anden art til borgerne via et informationssystem, hvorimod der formodentlig er langt færre aktører, der driver fjernsyns- og radioanlæg, ligesom disse kræver en offentlig tilladelse. Man kan evt. tale om en delvist gennemført kvalitativ afgrænsning af radio- og fjernsynsanlæg, hvorimod der ingen kvalitativ afgrænsning er sket i forbindelse med informationssystemer. Dette fordi informationssystemer, som sagt, kan tjene alle mulige roller, herunder til driften af alle andre anlæg, der er nævnt i § 193, samt alle mulige virksomheder og tjenester, store eller små, private eller offentlige, der ellers falder uden for bestemmelsen.

13.3.3 Afgrænsning fra straffelovens § 291 (hærværk)

Det er vigtigt at holde sig for øje, at § 193 ikke er en skærpet version af straffelovens hærværksbestemmelse. Bestemmelserne har forskellige beskyttelsesinteresser.

Som det også kom til udtryk i Carl Torps betænkning af 1917, kan man stille sig tvivlende over for, om der skulle være behov for særlig beskyttelse, ud over den eksisterende beskyttelse mod beskadigelse af fremmed ejendom, f.eks. i hærværksbestemmelsen (straffelovens § 291).[1117] Straffelovens § 193, som netop er placeret i kapitlet om andre almenskadelige handlinger, er da heller ikke en generel hærværksbestemmelse, men en bestemmelse, der beskytter mod omfattende forstyrrelser i driften af anlæg, der er uundværlige for borgerne. Det er vigtigt at være opmærksom på, at selvom en overtrædelse af § 193 nogle gange vil indebære groft hærværk (§ 291, stk. 2) udgør groft hærværk ikke nødvendigvis en overtrædelse af § 193. Der behøver tilsvarende heller ikke at foreligge hærværk for, at der kan ske en overtrædelse af § 193.

Også hærværksbestemmelses ordlyd er i det væsentligste uændret siden 1930, hvor den fik sin nuværende formulering. Bestemmelsen gør det strafbart at ødelægge, beskadige eller bortskaffe ting, der tilhører en anden. Stk. 2 omhandler hærværk af betydeligt omfang, eller af mere systematisk eller organiseret karakter samt tilfælde, hvor gerningsmanden tidligere er fundet skyldig efter visse bestemmelser. Bestemmelsen befinder sig i straffelovens kapitel om formueforbrydelser.

[1117] Carl Torps betænkning af 1917, mot. 168

Bestemmelsens bortskaffelseselement afgrænses over for § 276 om tyveri ved, at der ved anvendelse af § 291 ikke kræves forsæt til tilegnelse og dermed berigelse ved borttagelsen.

Ligesom i § 193, er midlet, som anvendes til at beskadige, ødelægge eller bortskaffe tingen uden betydning. Desuden er der ikke noget krav om, at tingen skal have nogen formueværdi. [1118] Der kræves heller ikke, at handlingen eller dens konsekvenser har haft en eller anden almenskadelig karakter, fordi bestemmelsens beskyttelsesområde er skader forvoldt på privat ejendom.

Databærende medier anses som ting. [1119] Der er ingen tvivl om, at hardware, der indgår i informationssystemer, udgør "ting" i § 291's forstand. Landsretten tager ikke direkte stilling til dette spørgsmål. Retten konkluderer dog under alle omstændigheder, at sletninger af og ændringer i data på et databærende medium udgør ødelæggelse af en ting, *når* denne sletning af eller ændring i data medfører, *"at de databærende medier ikke længere – i hvert tilfælde ikke uden særlige foranstaltninger – kan anvendes efter deres formål."* Der er et godt stykke fra denne konklusion til en konklusion om, at "data" i sig selv er "ting". Indtil videre foreligger der kun denne ene landsretsdom, der handler om data i en hærværkskontekst. Det er vel ikke udelukket, at domstolene i fremtiden vil nå frem til, at "data" er uløseligt forbundet med "ting" og tingens værdi. På nuværende tidspunkt, er U 1987.216Ø den eneste dom der forholder sig til, hvorvidt ændringen/sletning af data indebar "ødelæggelse" af en "ting" (nemlig, det databærende medium). Konklusionen i denne specifikke sag er ikke overraskende, da ændringer og sletning af data medførte, at den fysiske genstand ikke kunne anvendes efter dets formål.[1120] Dette punkt diskuteres ikke videre i denne artikel.

Som anført i det foregående afsnit, indebærer en overtrædelse af § 193 ikke nødvendigvis, at der også er sket overtrædelse af § 291 – eller omvendt. Man bør især holde sig for øje, at de økonomiske konsekvenser af enhver retsstridig handling mod et af de objektivt beskyttede anlæg i § 193, herunder informationssystemer, som udgangspunkt ingen relevans har for fortolkningen af begrebet "omfattende forstyrrelse". Disse økonomiske konsekvenser hører til gengæld hjemme i vurderingen af hvorvidt der er tale om hærværk eller groft hærværk[1121] (hærværk af betydeligt

[1118] Straffelovrådets betænkning nr. 1032/1985, s. 36
[1119] Jf. U 1987.216Ø, s. 219
[1120] Se også Mads Bryde Andersen: IT-retten (2005), s. 740 om § 291, s. 99 ff. om beskrivelsesproblematikken, samt s. 107 ff. om informationsteori, herunder den matematiske kommunikationsteori. Se endvidere om beskrivelsesproblematikken i Mads Bryde Andersen: EDB og Ansvar (1988), s. 50 ff.
[1121] Eksempelvis i U 1987.216Ø omhandlende ødelæggelse af programmel henførtes forholdet under § 291, stk. 2, da handlingernes indgribende karakter nødvendiggjorde indkaldelse af ekstern ekspertbistand. Se også U 2000.261Ø, hvor

omfang, jf. § 291, stk. 2).[1122] En forstyrrelse i driften af ethvert informationssystem kan eksempelvis kræve indkaldelse af ekstern ekspertbistand, hvilket ofte vil indebære betydelige omkostninger, men denne omstændighed er ikke noget, der relaterer sig til vurderingen af, hvorvidt systemet overhovedet er objektivt omfattet af § 193. Derimod har dette i retspraksis medført, at et forhold blev henført under § 291, stk. 2 (hærværk af betydeligt omfang).[1123] Økonomiske konsekvenser har i øvrigt aldrig indgået i den kvantitative vurdering (”omfattende”) i § 193, og dette var heller aldrig tanken. Denne økonomiske, kvantitative faktor hører til gengæld hjemme i § 291.

13.4 ”Omfattende forstyrrelse”

Samfundet er blevet afhængigt af informationssystemer, og der er også behov for beskyttelse af de vigtigste af disse. Imidlertid er ikke alle informationssystemer uundværlige for borgerne, selv når de har et stort antal brugere. I modsat fald ville Facebook[1124] være objektivt omfattet af § 193, da alene det danske brugerantal sandsynligvis er langt større end antallet af brugere af andre informationssystemer i Danmark. En fornuftig, kvalitativ afgrænsning bør foretrækkes, da der er alvorlige betænkeligheder ved for bredt et anvendelsesområde.

De eksisterende domme viser, at selv ganske kortvarige nedbrud i driften af anlæggene, så længe anlæggene kvalitativt er blevet vurderet som værende objektivt omfattet af bestemmelsen, kan opfylde kravet om ”omfattende forstyrrelse”, i kombination med brugerantallet. Det er endvidere klart, at forstyrrelsen, dvs. typisk et nedbrud i driften, skal kunne mærkes af borgerne. Ligesom forarbejderne tilsiger, er borgerne de subjekter, lovgiver forsøger at beskytte mod nedbrud i disse

---

hærværk til 10.000 kr. ikke kunne anses som værende af ”betydeligt omfang”. Hærværk til knap 295.000 kr. var hærværk af betydeligt omfang, jf. TfK 2011.668. Hærværk til 90.000 kr. og ”reelt uerstattelige værdier” var hærværk af betydeligt omfang, jf. TfK 2003.160.

[1122] Rigsadvokatens meddelelse nr. 9/2005 skalerende også strafpåstande i hærværkssager efter skadens økonomiske størrelse. Jf. meddelelsen skal forholdet henføres under § 291, stk. 2, hvis skadestørrelsen overstiger 15.000 kr.

[1123] Jf. U 1987.216Ø

[1124] I forslag til Europa-parlamentets og Rådets direktiv om foranstaltninger, der skal sikre et højt fælles niveau for net- og informationssikkerhed i hele EU COM/2013/48 nævnes sociale medier som markedsaktører, der skal være omfattet af direktivet. Det fremgår dog af Kommissionens impact assessment (SWD (2013) 32 final), s. 88, at man ikke anser sociale netværk for værende kritisk infrastruktur. Inklusionen af sociale netværk i direktivet (samt andre Internet services) er blevet kritiseret af Europa-parlamentet (http://www.europarl.europa.eu/oeil/popups/summary.do?id=1342725&t=e&l=en) samt i komité rapport (http://www.europarl.europa.eu/oeil/popups/summary.do?id=1337255&t=e&l=en). Kommissionen, i dennes svar på Europa-parlamentets ændringsforslag, kunne kun acceptere nogle af forslagene (http://www.europarl.europa.eu/oeil/spdoc.do?i=24217&j=0&l=en).

samfundsvigtige systemer, der er uundværlige for borgerne. Bortset fra én enkelt byretsafgørelse[1125], er bestemmelsen indtil videre fortolket således, at den ikke omfatter nedbrud af informationssystemer eller andre beskyttede anlægstyper, der kun påvirker "interne brugere" og dermed aldrig rækker så vidt at ramme den almindelige borger.[1126] Forstyrrelsen skal også i øvrigt være realiseret, og ikke blot være potentiel[1127]. Dette er også i overensstemmelse med det i forarbejderne beskrevne anvendelsesområde.

Antallet af brugere har selvfølgelig fået en fortjent plads i domstolenes vurdering af, hvor omfattende forstyrrelsen i driften af anlæggene har været. Men man bør have in mente, at når brugerantallet indgår i vurderingen af, hvor omfattende forstyrrelsen har været, har det altid været i forbindelse med sager, der er baseret på forstyrrelser i driften af anlæg, der i forvejen er blevet kvalitativt vurderet som værende omfattet grundet deres funktion, så som vandforsyning. Det vil sige, at de beskyttede anlæg grundet deres specifikke samfundsrolle, fx vandforsyning, elforsyning eller lignende, allerede er kvalitativt afgrænset til reelt samfundsvigtige anlæg. Som også fremhævet i det ovenstående, har informationssystemer vidt forskellige roller i samfundet, og de færreste burde være omfattet af § 193, uanset at nogle har flere millioner brugere. I en sag omhandlende vandforsyning[1128], havde den tiltalte skåret en vandledning over, hvilket bevirkede, at et landsbyssamfund på ca. 80 husstande og ca. 15.000 husdyr var uden vand i flere timer. I en anden sag[1129], der dog endte med frifindelse grundet fravær af grov uagtsomhed, havde forurening af drikkevand gjort ikke mindre end 150 personer syge, og forureningen havde påvirket forsyningen af drikkevand til ca. 7.000 borgere. Ligeledes i en førnævnt dom[1130] omhandlende afbrydelse af udsendelsen af TV-avisen, lagde retten vægt på, at der var tale om en landsdækkende kanal, at der var tale om et program med et meget stort antal seere, samt at afbrydelsen ikke var helt kortvarig (ca. 20 minutter).

[1125] Dom afsagt af Retten i Roskilde 19.december 1996, der omhandler hacking af en række systemer i forskellige lande, herunder amerikanske militære systemer. Det forslåede direktiv vil, i sin nuværende form, ikke blot dække kritisk infrastruktur men også andre markedsaktører.
[1126] Se fx U 2002.2700V hvor der ganske vist manglende forsæt til overtrædelse af § 193, men hvor retten endvidere konstaterede, at forstyrrelsen faktisk ikke var realiseret, selvom om potentialet for en forstyrrelse havde været til stede.
[1127] U 2002.2700V. Forsøgsstraf er selvfølgelig en mulighed, hvis der er forsæt til den realiserede forbrydelse.
[1128] U 2005.1357V
[1129] U 2011.1144Ø
[1130] U 2001.1187Ø

Forvirringen angående informationssystemer viser sig i en af de to hackerdomme omhandlende forstyrrelse af informationssystemer, som er en utrykt byretsdom[1131] fra 1996. Sagen, som nok kan beskrives som den største hackersag i Danmark før CSC-hackersagen,[1132] omhandlede bl.a. hacking af informationssystemer ejet af den amerikanske regering. Retten nåede frem til, at ét af systemerne, tilhørende det amerikanske militær, var objektivt omfattet af § 193, ligesom et andet system, tilhørende den amerikanske vejrtjeneste, der tjente operationelle formål, også ansås som omfattet af bestemmelsen. Derimod var der to andre systemer, ligeledes tilhørende den amerikanske vejrtjeneste, der tjente udviklings- og forskningsformål, der af retten ikke blev anset som værende objektivt omfattet af § 193. Retten fandt den tiltalte skyldig i overtrædelse af § 193, for forstyrrelsen i driften af systemet tilhørende det amerikanske militær, på trods af at de 5.000 brugere var militærets "interne brugere". Retten fandt, som nævnt, at også forstyrrelsen i driften af den amerikanske vejrtjenestes operative system, var omfattet af § 193. Dette sidste forekommer mere oplagt, idet systemet leverede vejroplysninger, der bl.a. modtoges mere eller mindre direkte af borgere og kunne have væsentlig betydning for dem. Slutteligt fandt byretten den tiltalte skyldig i forsøg på overtrædelse af § 193 for forstyrrelsen i driften af de to forsknings- og udviklingssystemer, tilhørende den amerikanske vejrtjeneste, som retten allerede havde konkluderet ikke var objektivt omfattet af bestemmelsen. Rettens begrundelse for den del af afgørelsen, der relaterer sig til de ikke-objektivt omfattede systemer, var, at tiltalte vidste, *a*t der var tale om regeringscomputere, selvom han ikke vidste, at de tilhørte den amerikanske vejrtjeneste eller kendte deres rolle, *at* tiltalte var klar over, at der var tale om computere med særlig stor regnekraft, og *at* tiltalte havde accepteret konsekvenserne af sine handlinger.

Bortset fra det led, der omhandler vejrtjenestens operationelle systemer, er det ikke nemt at forstå hvordan afgørelsen harmonerer med forarbejderne. I forarbejderne fremgår det af eksemplerne på beskyttede systemer, at det forhold, at en computer er en regeringscomputer, netop ikke i sig selv skaber en formodning om, at systemet objektivt er omfattet af § 193. Selvom der ikke er formodning for, at regeringsejede systemer er objektivt omfattet af § 193, er angreb mod

[1131] Utrykt byretsdom afsagt af Retten i Roskilde, 19.december 1996. Omtalt i eksempelvis bet. 2002/1417.
[1132] Den 30.oktober 2014 afsagde Retten på Frederiksberg dom i CSC-sagen. De tiltalte blev frifundet for overtrædelse af § 193, idet der ikke var sket "nedbrud eller andre betydelige forstyrrelser i driften hos CSC som følge af angrebet." Landsretten frifandt også T1 for overtrædelse af straffelovens § 193. De ændringer, der blev foretaget i systemet i forbindelse med hackerangrebet havde ikke fremkaldt omfattende forstyrrelse i driften af systemerne. CSC's kunders økonomiske tab ifm. periodevis lukning af systemerne med henblik på at patche systemerne udgjorde heller ikke en omfattende forstyrrelse i driften af systemerne. Se Østre Landsrets afgørelse afsagt 17.juni 2015, s. 2.

regeringssystemer i forarbejderne[1133] nævnt som et eksempel på skærpende omstændigheder, som straffelovens § 263, stk. 3 (uberettiget adgang under skærpende omstændigheder) sigter mod. Strafferammen er i øvrigt identisk med strafferammen i § 193.

Det må derfor særligt undre, at tiltalte blev fundet skyldig i forsøg på overtrædelse af § 193 i realiteten alene af den grund, at han var klar over, at der var tale om en regeringscomputer, og at computeren havde særlig stor regnekraft, selvom systemet altså ikke objektivt var omfattet af § 193, og selvom han ikke – bedømt efter rettens egne præmisser – havde forsæt til at volde omfattende forstyrrelser.

I CSC-sagen stod det klart allerede før de pågældende personer blev sigtet, at der ikke var sket en konkret forstyrrelse i driften af selve informationssystemet. Et af anklagemyndighedens vidner, som var ansat hos CSC (kaldt vidnet G i afgørelsen) forklarede i retten, "at der ikke var nedbrud eller andre betydelige forstyrrelser af driften hos CSC som følge af angrebet."[1134] Alle nødvendige fejlrettelser var allerede foretaget den 6. marts 2013 uden at der var sket nedbrud. I juni 2013 blev de senere tiltalte alligevel sigtet for bl.a. overtrædelse af straffelovens § 193 i forbindelse med angrebet på CSC. Anklagemyndigheden forklarede den første retsdag[1135] ikke rigtigt hvori forstyrrelsen i driften lå, men forklarede alene, at der ved anvendelsen af § 193 skal tages hensyn til antallet af berørte personer. De berørte personer, mente anklagemyndigheden, var alle borgere i Danmark, i og med at angrebet involverede uberettiget adgang til CPR-registret, og at uddrag fra CPR-registret muligvis var blevet videregivet til andre personer (uden at dette dog på noget tidspunkt blev bevist under retssagen). Det er klart, at anklagemyndigheden har løsrevet to uløseligt forbundne begreber, nemlig "omfattende" og "forstyrrelse i driften" af informationssystemet. Ud fra sagens fakta, som forelå, allerede før de tiltalte blev sigtet, var det klart, at straffelovens § 193 ikke var overtrådt, fordi der ikke var fremkaldt en forstyrrelse i driften af systemet. Det var følgelig ikke relevant at tage stilling til størrelsen af den berørte personkreds, som kun ville indgå i vurderingen af, om en konkret forstyrrelse faktisk var "omfattende". Et abstrakt risikomoment forbundet med et potentielt efterfølgende misbrug af CPR-numrene er ikke foreneligt med ordlyden af straffelovens § 193, der kræver (hvor der ikke er tale om forsøg), at forstyrrelsen er realiseret – ikke blot

[1133] KBET nr. 1032/1985, s. 79

[1134] Se afgørelsen af skyldspørgsmålet i sagen på rettens hjemmeside: http://www.domstol.dk/frederiksberg/nyheder/domsresumeer/Pages/Afg%C3%B8relseafskyldssp%C3%B8rgsm%C3%A5letisagomhackingafCSC.aspx

[1135] Den 2.september 2014. Forfatteren var til stede i retten.

potentiel.[1136] Derudover synes anklagemyndigheden at have løsrevet "forstyrrelsen" fra "driften" af selve systemet, da usikkerheden forbundet med en mulig videregivelse af CPR-numre i sig selv er irrelevant for informationssystemets fortsatte uforstyrrede drift. Baseret på den ovenfor omtalte vidneforklaring om, at der ikke var sket forstyrrelse i driften af systemet, frifandt byretten da også, som nævnt, de tiltalte for overtrædelse af straffelovens § 193.[1137]

Det man kan udlede af retspraksis er, at forstyrrelsen i driften af systemet skal være realiseret og ikke kun være potentiel. Desuden skal forstyrrelsen være omfattende, hvilket tager hensyn til antallet af påvirkede borgere. Dette er i overensstemmelse med forarbejderne, da den omfattende forstyrrelse skal være almenskadelig.

13.5 Afsluttende bemærkninger

Domstolene har ikke fået en nem rolle, i og med de skal forsøge at forene forarbejderne med tilføjelsen af det tilsyneladende altomfattende begreb "informationssystemer" i § 193. Som Vagn Greve også har påpeget,[1138] så er det ikke nok, at virksomhedens eller myndighedens "interne brugere" er påvirkede. Der skal mere til for at nå op på det "almen*skadelige* niveau" – og her bør det fremhæves igen, at der netop ikke er tale om "almen*farlige* handlinger". Konsekvenserne af at sige, at den kvalitative vurdering baseres på en kvantitativ vurdering, er det samme som at sige, at alt, der kan tælles, tæller. Det er dog indlysende, at dette aldrig har været var meningen med § 193, da man netop lagde afstand til det næsten "alt-inkluderende" 1912-forslag til bestemmelsen, og positivt valgte at afgrænse de beskyttede anlæg til dem, man anså for værende uundværlige for borgerne. Ikke alle informationssystemer er skabt lige, og de færreste af dem vil i bund og grund være uundværlige for borgerne i forarbejdernes forstand. Selvom vi bor i et forholdsvis rigt land med en høj levestandard, må man være påpasselig med at udvande betydningen af "uundværligt", især når dette ord indgår i fortolkningen af en meget alvorlig bestemmelse i straffeloven.

[1136] Det kan yderligere diskuteres, hvorvidt sådan en fortolkning ville være forenelig med artikel 7 EMRK, der udtrykker princippet om nullum crimen sine lege. I sagen *Liivik mod Estland* konstaterede Menneskerettighedsdomstolen i Strasbourg, at en straffebestemmelse, der efter sin ordlyd kræver at skaden er realiseret, ikke kan fortolkes udvidende således, at den også omfatter den blotte risiko for skade. Se *Liivik mod Estland*, dom af 25.september 2009, § 99.

[1137] Se afgørelsen af skyldsspørgsmålet i sagen på rettens hjemmeside: http://www.domstol.dk/frederiksberg/nyheder/domsresumeer/Pages/Afg%C3%B8relseafskyldssp%C3%B8rgsm%C3%A5letisagomhackingafCSC.aspx

[1138] Vagn Greve: EDB-kriminalitet (2. Rev.udg. 1986, s. 24)

Antallet af de påvirkede brugere (andre end myndighedens eller virksomhedens egne interne brugere) indgår i vurderingen af, hvor "omfattende" forstyrrelsen rent faktisk har været, men dette er ikke det samme som at lade antallet af berørte brugere være det eneste vurderingskriterium når det skal afgøres, hvorvidt et system overhovedet er omfattet af § 193. Antallet af påvirkede borgere alene var under alle omstændigheder ikke nok til at fortolke begrebet "almindelige samfærdselsmidler" så bredt, at det omfattede privatbilismen.[1139] Der er grund til at afvise at anvende § 193 i sager, hvor der nok er tale om angreb på regeringssystemer, men hvor virkningerne kun føles "internt". Der er en række andre bestemmelser i straffeloven, der kan omfatte sådanne angreb. Nævnes kan fx § 263, stk. 2 og stk. 3 (hvor der ikke nødvendigvis er sket en forstyrrelse, men hvor gerningsmændene har været inde i systemet), § 291, stk. 1 og stk. 2 (hvor gerningsmændene har forvoldt skade) og/eller § 293, stk. 2 (hvor gerningsmændene har forårsaget elektronisk rådighedshindring). § 263, stk. 3, jf. stk. 2 og § 291 stk. 2, har i øvrigt den samme strafferamme som § 193. Det er derfor svært at finde noget godt argument for at anvende en så udvidet fortolkning af § 193, som en ren kvantificering af kvalificeringen giver anledning til.

[1139] U 1986.423/2 Ø

14 CONCLUSION AND FINAL REMARKS

The Danish hacking provision turned thirty years old this year. Yet, it has not undergone much development in terms of exploration and clarification of its scope. Granted, for half of its life computers were not a household commodity and the pool of possible defendants was relatively small. In later years, computers can be found in almost every home, internet access is widespread and cheap, and information is shared globally through interlinked sites on the world wide web. Today, computers are so small that we can wear them on our wrists or carry them in our pockets, and a world of information is available to us at the press of a button. But we heavily rely on computers and networks of other people moving our packets around and hosting information and services, all of which necessarily necessitates accessing computers, programs and information belonging to others at a grand scale that the legislature in 1985 could not have anticipated. Global resource and information sharing is vital to our modern society and we rely heavily on access to computers, programs and information belonging to others for research, hobbies, day-to-day communications, business, government, education, news reports and much more.

Both the Danish and the US statute grew out of traditional trespass theories.[1140] The Danish hacking provision is rooted in a chapter on privacy violations (which includes trespass), and forms a subsection of a provision that is aimed at protecting information, chattels and communications, rather than forming a part of the trespassing provision aimed a buildings, land property, etc. This makes it tempting liken a computer to a residence and then apply whatever norms have already been established with respect to private residences. For example, by giving an owner an almost absolute right to exclude e.g. competitors from public websites simply by telling them directly that they are unwelcome and would be trespassing if they would access the public website which is hosted on a computer that is private property. Is it really possible to liken such "trespass" with trespass onto physical property? In terms of a public website there is no privacy to protect, a competitor or other unwanted visitor visiting the website along with perhaps thousands of other users who are generally completely unaware of each others "presence" on the website, and making the website publicly accessible a choice as long as there is no law that mandates making the information publicly accessible. Someone physically entering onto your private property is much more intrusive, because it is impossible for you to "disconnect" your physical property from the surrounding world such that

[1140] See Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, pp. 1596-1668, p. 1617-1619 and see also the Danish Committee Report, 1985 no. 1032 and e.g. the US Committee report S. Rep. 99-432

it would impossible for others to enter it, and it was not your choice to "connect" it to the world in the first place. Furthermore, the norms developed in connection with trespass in the physical world are heavily reliant on what signals we get from the environment. We instinctively know, in most cases, whether a building is a private residence, commercial property, government building, and know from experience with norms whether we need prior permission to enter or not. Even if all these buildings belong to others, we know that different rules apply. Trespass statutes are generally broad and do not explain as such when access is authorized or unauthorized, and they do not state that we need prior permission in some cases but not in others. If we disregard these and other differences and blindly follow the norms associated with physical trespass, the results are likely to be odd and impractical. The computer environment is different, especially online, and there is not yet a broad, common understanding of what in the environment signals a closed off area and what signals an open area. Recall again the *Explorica* case. The circumstances that the plaintiff relied on as indications that the defendant's access was unauthorized would require a user to interpret a copyright symbol as a signal that he must ask permission to use information that is not covered by copyright law, as well as interpreting the presence of hyperlinks as excluding any other method of browsing. There is no such common understanding relating to copyright symbols and hyperlinks, and thus, it would be arbitrary and unforeseeable to choose these circumstances as legally relevant facts that indicate lack of authorization to access.

There is little guidance in the statutory language and the legislative history with respect to when access is unauthorized, apart from using passwords not belonging to oneself. The Framework Decision and the Directive appear to refer back to domestic law with respect to determining the meaning of "without right". The Convention's explanatory report also refers back to domestic law[1141], but adds that access to systems that allow free and open access by the public is with right. This is not reflected in the statutory language of either the Danish or the US provisions, nor is it reflected in the Council's Framework Decision on attacks against information systems or directly in the EU Directive that repealed and amended the Framework Decision. The Directive makes it mandatory to limit the scope of implementing illegal access provisions to those cases where security measures were circumvented in order for access to be gained. However, it is regrettably unclear what constitutes a security measure under the Directive, which leaves the door open for inclusion of "barriers" that are based on client-side controlled information e.g. IP addresses, cookies, user-agent

[1141] See also Russell G. Smith, Peter Grabosky and Gregor Urbas: Cyber Criminals on Trial (2004), p. 104

strings and other factors that are completely within the user's power to change, and often are changed or modified for e.g. privacy or research reasons.

The Directive has taken what is arguably a code-based approach, and it inherits the flaws and inconsistencies of a pure code-based approach that have been revealed through the years in US case law and literature. The preamble of the Directive explicitly rejects a contract-based approach as well as an agency-based approach – at least were a breach of contract or labor dispute is the sole basis for claiming that the access was unauthorized. These are the approaches that have been subject to harsh criticism from courts and commentators in the US, since the approaches often involve automatic revocation of authorization based on the motive for the access which is otherwise authorized; e.g. breaches of terms of use (public website's and employer's terms) and motives that are contrary to the interest of the employer (disloyalty). Although the contract-based approach is still applied in several jurisdictions in the US, it is entirely unclear if all breaches of contract relating to the access to or use of a computer are criminal or if it is just some breaches that are criminal. If all breaches are criminal, then it is effectively the computer owners who define the scope of hacking statutes. If only some breaches are criminal, the question becomes which ones are criminal, and how can the courts provide the sufficient foreseeability and protection against arbitrary enforcement if it is now foreseeable which breaches trigger criminal liability. Since policies are generally unilaterally drafted and issued and may be changed without notice, this again makes them suspect as a basis for determining lack of authorization. Furthermore, the content of terms of use/service and other policies can be very vague, such as Facebook's terms that prohibit violating the spirit of the terms or employer policies prohibiting non-business uses. In such cases, one would first have to interpret the vague terms the violation of which supposedly trigger criminal liability. Additionally, courts would have to be wary of written policies that do not reflect the actual organization culture; e.g. where the written policies are neither complied with or enforced, but may nonetheless be called upon as a basis for the purposes of establishing lack of authorization to access – i.e. arbitrary enforcement of the terms. Finally, breaches of contract do not automatically discharge the contract (and thus, the authorization). A party must notify the party in breach that he is avoiding the contract due to the breach. The wronged party may not even necessarily be entitled to avoid the contract if the breach is not considered fundamental. Then the wronged party must explore what other less extreme remedies are available to him.

For all of the above reasons, the contract-based approach gives cause for concern if adopted by Danish courts.

The agency-based approach has not been widely adopted in the US. It is extremely plaintiff-friendly, and typically had been used to target trade secret violations based on the argument that the purpose of the access was contrary to the interests of the employer; the defendant automatically ceases to be an agent of the employer when he accesses the information he is generally authorized to access, but does so for reasons that are disloyal to his employer. In other words, the planned subsequent unauthorized use or disclosure of trade secrets supposedly convert an authorized access into unauthorized access. This approach to construing unauthorized access statutes can only be applied in the employer-employee context. Such an approach has ostensibly been rejected in the Danish case *U 1996.979 Ø*, albeit absent explicit references to disloyalty and possible trade secret law violations. Here the High court rejected letting the purpose of the access negate the fact that the defendant was authorized to access the information. The court did not provide extensive reasoning for its conclusion, but laconically stated that at the time the defendant was an employee and thus had authorized access to the information. The court did not explain why it implicitly rejected the prosecution's theory. However, the conclusion appears correct – especially given that the information were not confidential with respect to the defendant as he had full authorized access, and the objectionable conduct clearly related to the alleged intention to disclose the information to a competitor.[1142] Since disclosure and use of information are not covered by the Danish hacking statute, it is inappropriate to construe it as triggering criminal liability simply by restating that later disclosure or use rendered the authorized access unauthorized due to the motive. This of course is not an argument against protection of trade secrets or other confidential information. These information are already protected by criminal sanctions, and there is no justification for judicially expanding the scope of the hacking provision beyond "access" to include future use of information. The legislature has proven itself perfectly capable of phrasing statutory language in terms of purpose, use of information and disclosure of information – it did not do so in either the CFAA, the Danish § 263(2), the Convention, the Framework Decision or the Directive.

The social norms approach has not been mentioned by US courts as a specific approach. The approach is largely derived from the Second Circuit's decision in *US v. Morris*, which covered various conduct the means of access and context of which the court relied on to determine whether the access was unauthorized or not. The usefulness of the court's decision in *Morris* becomes clearer when compared to other approaches developed through US case law over the years and as

[1142] See opposite opinion in Mads Bryde Andersen: IT-retten (2005), p. 746

the weaknesses of the other approaches become apparent through aggressive prosecution and civil litigation.

It is true what the Australian court said; that computers cannot authorize anything. However, now we live in a world where the majority of our authorization to access computers belonging to others relies on tacit consent. The Convention's explanatory report states that maintaining a public website implies consent. In other words, given the open nature of the Internet, if one desires to limit access to a website, one should take steps to "close" that particular space in order to be able to specifically authorize those allowed to access and keep the rest out. Code defines the space to a significant extent and also defines how it is possible to access information. Code signals what is closed and what is open on the Internet, for example. However, the code-based approach is too narrow in the sense that it fails to reach conduct that we all agree is unauthorized access (such as guessing passwords, without permission, to gain access to accounts that do not belong to us) but code nonetheless does not prevent.

Since code defines the nature of the space and how it can be accessed, code is not irrelevant either, even though the code-based approach needs some adjustments. In a draft paper dated May 2015, Orin Kerr recognized this weakness in the code-based approach, for which he had previously advocated. He proposes a social norms approach that appears to be rooted in code, thus, in a way patching the vulnerabilities and bugs of a pure code-based approach.[1143] This approach entails the analysis of three factors; 1) the nature of the space, 2) the means of entry/access, and 3) the context of entry/access. For example, if the space is open, such as a public website, there is presumably no criminal protection against access to the public-facing parts of the website. The context of the entry should not be understood as an inquiry into the purpose of entry of a person who is authorized to access, but does so for objectionable reasons. Rather, the context can clarify the meaning of authorization where there person would generally be unauthorized to access, but does so for a

[1143] The code-based approach was initially understandably attractive in comparison to the contract and agency approaches. Over the years, several courts have cited Kerr's work in which he argues in favor of a code-based approach. But in the last several years, Kerr's ideas of relying on code to determine authorization saw some, perhaps unexpected, applications, as courts began interpreting code restrictions to encompass barriers that relied on IP address blocking, user-agent strings, cookies and so on. Ostensibly, these restrictions bear not even a passing resemblance to the code restrictions Kerr seemingly envisaged in his 2003 "Cybercrime's Scope" article. In other words, it must have become apparent to Kerr, as it became apparent to me – particularly in light of US v. Auernheimer (2014) (he represented the defendant on appeal), Craigslist v. 3Taps (2013), and US v. Lowson (2010), that the code-based approach could be turned to serve interests that have little or nothing to do with the protected interests at the heart of hacking statutes, and more to do with protecting the bottomline by keeping out direct or indirect competitors, or to serve as tools for aggressive prosecution.

socially recognized purpose, such as the mailman entering the property to deliver the mail, or where a person who is not authorized but does not gain access through objectionable means, e.g. a person guessing a password to access a closed space (without the means of access being suspect as such, i.e. against the intended function) under circumstances where no delegation of authority from the owner has taken place. The social norms-approach is not free from consideration of code. In fact, code inherently defines the nature of the (virtual) space, because the code provides the framework for the space (whether it is open or closed) and thus naturally influences the social norms that will later attach themselves to that particular space. Furthermore, code provides the framework for the means of access. However, code free from interpretation as a legal basis for a criminal conviction will produce absurd and arbitrary results, and hence, results that are irreconcilable with social norms; including both cases where the conduct was clearly unauthorized even though the code did not prevent the access, and cases where code (perhaps contract-inspired) arbitrarily triggers criminal protection of use of and access to publicly accessible information. The social norms approach can be said to correct and amend the code-based approach in that the social norms approach does not disregard code but injects some common sense and foreseeability into the analysis of authorization in a virtual environment as well as reducing, to some extent, the risk of arbitrary enforcement compared to the risks associated with a pure code-based approach and the contract-based approach. However, a social norms approach, if construed too liberally, can drastically increase the risk of arbitrary enforcement and reduce foreseeability if social norms are widely construed to mean e.g. "courteous" conduct or construed as prohibiting "annoying" conduct. Therefore, it is important to remain focused on the three prongs related to the *access*; not on the purpose of the access where access is generally authorized, or on the subsequent use of information obtained through the otherwise authorized access etc. Thus, ultimately, what matters is whether society recognizes the computer owner's expectations of protection against trespass; hence, barring indiscriminate, surprising and/or arbitrary criminal enforcement of ambiguous, broad statutory language that may be at odds with the constitutional and/or human rights related to due process, clarity of criminal law provision, etc. The social norms in the computer context need time to develop; norms related to traditional trespass did not develop overnight. The space, particularly the virtual space, associated with computers and networks is different from physical space. Simply indiscriminately transferring traditional trespass rules into the computer context, by relying on (often inappropriate or inaccurate) analogies, ignores the differences between the spaces.

Efforts have been made to rein in the broad scope of hacking statutes in both the EU and the US. In the US, a bill popularly known as *Aaron's Law*[1144] was proposed in 2013. The bill proposes several amendments to title 18 USC, one of which serves to exclude from *unauthorized access* situations where the access is in violation of terms of service and user policy agreements with online service providers, Internet websites or employers, and situations where access was gained by proxy server, or by the user preventing identification of user hardware or software.[1145] And as mentioned earlier, the preamble to the EU Directive suggests a similar narrowing of the scope of illegal access, combined with the mandatory requirement that illegal access must have been gained by circumvention of a security measure.

The social norms approach implies that circumvention of security measures is generally needed, but also recognizes that there are contexts, such as where a random visitor in an office building accesses an unprotected computer without ever having been authorized and thereby obtains information, and yet he is not hindered by code. Neither the contract-based approach nor the agency-based approach would be able to catch this type of unauthorized access either.

Where circumvention of security measures is required to trigger criminal liability for unauthorized access, the courts' construction of "security measures" becomes critical to the scope. If "security measures" are interpreted to mean "code barriers" more broadly, IP address blocking, and similar efforts that rely on information the user has full control over and is free to change, cookies and so on, may be considered "security measures" by the courts.

Recall the cases involving URL hacking that are discussed above in the chapter on outsiders. In cases where companies accidentally make personal information publicly accessible through minor changes in the URL, these companies might face fines in the millions of euro under the coming EU Data Protection Regulation. Thus, more cases will likely arise, when the EU's General Data Protection Regulation enters into force, in terms of URL hacking that has led to discovery of security vulnerabilities, because the proposed fines for non-compliance (including failing to

[1144] Proposed in memory of Aaron Swartz, a target of federal hacking prosecution who committed suicide before the trial started. The text of the proposed legislation can be found on the World Wide Web at http://thomas.loc.gov/cgi-bin/query/z?c113:H.R.2454:. accessed June 23rd 2014. The bill was stalled in committee, but was reintroduced in 2015. Available at Senator Ron Wyden's (D-Ore.) Senate webpage at https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-. Last visited on 26 August 2015.

[1145] Suggested amendments to section 1343 of title 18 United States Code.

implement security) are based on the company's annual global turnover[1146] – meaning the fines will be dramatically higher than at present time – and companies may possibly be less forgiving and less willing to consider discoveries and reporting of vulnerabilities that involve personal data exposures "helpful suggestions". The companies' only defense strategy to attempt to avoid the hefty fines might arguably be to claim they have been "hacked" – that is, that the access to unintentionally accessible information was unauthorized, because URL hacking, under a creative reading of "security measures" does not technically distinguish itself from password guessing, regardless of the fact that "secret" URLs are a poor password-analogy given their intended function as web addresses (resource locators).

Also, as importantly noted by numerous US federal courts, Marco Gercke (in the context of the Convention on Cybercrime and several domestic legal systems), Orin Kerr, and others, it is imperative to separate the *access* from *subsequent conduct* (typically, this is accomplished by inquiring into the purpose of the access) that is either illegal and/or a breach of contract. This problem is only relevant where the defendant had implicit or explicit authorization to access and this is sought to be negated by later conduct. Allowing other legal rules concerning subsequent acts to negate authorization opens up the scope of hacking statutes giving them enormous reach. For example, access to information for the purposes of using the information in violatation of any law would automatically also trigger liability under the hacking statute. This would make breaches of data protection law, copyright law, trade secret laws and other laws regulating use of information, such as processing personal data in excess of what is necessary and online piracy, etc. Furthermore, it would allow constructions such as that from *US v. John*, where a person with authorized access was nonetheless convicted of unauthorized access, because she intended to use the information to commit fraud. These illegal acts are not related to *access* to information, but the subsequent *use* of information. Rather the access, in combination with other facts, may be indicative of an attempted crime that directly prohibits a specific use of information, such as disclosure of trade secrets, or where the information is used to commit other crimes, such as fraud.

All in all, it can be said that the harmonization to which the Convention on Cybercrime aspired is largely symbolic. The broad and imprecise language of the illegal access article is primarily owed to

[1146] See proposal for the General Data Protection Regulation at the legislative observatory at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212. See specifically article 79 on the fines for non-compliance with the regulation.

the main supposed limitation of the criminalization, namely the term "without right". When the legal meaning of the defining term of the article is practically entirely left to be determined in domestic law, it is no wonder that national courts, even within the same legal system, cannot agree on its meaning and consequently on the extent of criminalization. Thus, whereas in some jurisdictions one may commit a crime by violating terms of service of a website, the same conduct is legal elsewhere – even if the language of the statutes is identical or very similar, and implements the same Convention.

The hacking statutes are unlikely to violate the void-for-vagueness doctrine or article 7 ECHR *facially*, because both the US Supreme Court and the ECtHR allow broad statutes that are clarified in through case law. However, the various approaches to construing hacking statutes can seemingly render the statutes incompatible *as applied*, if the application was not reasonably foreseeable and/or if the application was arbitrary. Thus, the need for clarification of broad hacking statutes.

15 ABSTRAKT PÅ DANSK

I år er det tredive år siden den danske hackerbestemmelse blev vedtaget. Allerede den gang var man bevidst om, at bestemmelsens ordlyd var egnet til at fange flere forhold end nødvendigt for at opnå bestemmelsens formål. For at stemme op om et ellers alt for bredt anvendelsesområde, indsatte man ordet "uberettiget". Begrebet "uberettiget" skulle medføre, at domstolene var bevidste om, at der var straffri forhold, der kunne falde inden for ordlyden, og dermed gøre dem opmærksomme på, at de var nødt til at foretage en konkret vurdering i hver sag. Dette svarer i princippet til straffelovens andre bestemmelser om fredskrænkelser. Det interessant er, hvordan domstolene kan eller burde udøve dette skøn i forbindelse med bestemmelsens anvendelse.

Bestemmelserne om freds- og æreskrænkelser er generelt meget brede og deres indhold følger ikke klart alene af bestemmelsernes ordlyd. De andre bestemmelser anvendelse, fx straffelovens § 264 om uberettiget adgang til fremmed hus, er bygget på flere hundrede år af normudvikling, der delvist præciserer indholdet af § 264, og gør anvendelsen af bestemmelsen mere eller mindre forudsigelig i de fleste tilfælde. Vi ved af erfaring og sociale normer, at vi ikke blot kan gå ind i et privat hus, og vi må afvente invitation til at komme indenfor. Men hvad der konstaterer et privat hus, og dermed hvornår en særlig invitation er nødvendig, er noget vi fornemmer og udleder fra vores omgivelser; bestemmelsen beskriver ikke hvad et privat hus er, og beskriver derfor hverken hvornår man kun må komme indenfor hvis man er inviteret eller hvilke undtagelser der måtte gælde hertil. Men det er ikke en overtrædelse af § 264 hver gang vi går ind i "fremmed hus" uden særlig tilladelse, fordi der er signaler fra vores omgivelser, der indikerer, at andre regler gælder fx når vi skal ud at handle i et supermarked. Her ved vi ud fra erfaring og ud fra signaler fra omgivelserne, at vores adgang til fx et supermarked, selvom det er fremmed hus, ikke er uberettiget – også selv om vi ikke har modtaget en særlig indbydelse til at komme indenfor. Men som sagt, dette er intet der følger af bestemmelsens vage ordlyd, og domstolene udtrykker heller ikke hvorfor disse normer er som de er (hvilket der måske heller ikke er behov for i forhold til fremmed hus – men grundet at normerne i forhold til computere stadig er uklare, er det vigtigt at forstå domstolens rationale).

I 1985, da straffelovens § 263, stk. 2 blev vedtaget, var der ikke nogen bred erfaring med computere i samfundet. I midten af 90erne var det ikke længere så ualmindeligt at eje en computer. Dette samt at adgang til internet og world wide web blev mere tilgængeligt for befolkningen indebar også at antallet af handlingerne som kunne blive omfattet af bestemmelsen blev forøget. Især Internettet og world wide web, som jo direkte indebærer adgang til andres informationer og programmer,

krævede, at man tog stilling til hvornår adgang så var uberettiget. Det rejser utallige spørgsmål i forhold til fortolkningen af § 263, stk. 2, fordi er vi har ikke haft særlig lang tid til at finde ud af hvilke normer der gælder på internettet og generelt i forhold til computere; dvs. hvornår adgang er uberettiget og hvornår den er berettiget, om der kræves særlig invitation, eller hvilke signaler indikerer, at et område er frit tilgængeligt og derfor ikke kræver særlig invitation.

Selv i de tilfælde, der omhandler ansatte og deres adgang til arbejdsgiverens computere og netværk, er det ikke klart hvilke handlinger udgør overtrædelse af bestemmelsen. Denne usikkerhed var allerede udtrykt af straffelovrådet i 1985 i betænkning nr. 1032/1985.

Desværre er der få afgørelser omhandlende overtrædelser af straffelovens § 263, stk. 2, og de få der eksisterer er, med en enkelt undtagelse eller to, sager der utvivlsomt udgjorde overtrædelse, eller forsøg på overtrædelse, af § 263, stk. 2; eksempelvis forsøg på at skaffe sig adgang til en andens computer ved brug af kendte hackerværktøjer med henblik på at omgå sikkerhedsforanstaltninger. Desuden beskriver danske domstoles afgørelser, som bekendt, sjældent særlig udførligt hvordan domstolene nåede frem til deres konklusion, hvilket gør det svært at analysere afgørelserne med henblik på at udfinde principper eller en analyseramme, der kan bidrage til forudsigeligheden af anvendelsen af en bestemmelse med et ret uklart, og potentielt utrolig bredt, anvendelsesområde.

Domstolene er blevet pålagt at udøve skøn i forbindelse med anvendelsen af en bestemmelse til hvilken forarbejderne mildest sagt tilknytter meget sparsom vejledning. Domstolene sidder foran en svær opgave, der selv i 1985 var upræcis, trods at computere dengang ikke var almeneje og der ikke var udbredt åben adgang til andres informationer og programmer. Deres opgave er under ingen omstændigheder blevet forenklet ved tilkomsten af udbredt internetadgang og brug af world wide web, der forudsætter adgang til andres information og programmer, hvorfor fortolkningen af ”uberettiget” bliver afgørende for rækkevidden af kriminaliseringen i § 263, stk. 2.

Heldigvis er Danmark ikke det eneste land, der har indført en bredt formuleret hackerbestemmelse. De amerikanske føderale domstole har flere års erfaring med anvendelsen af en bestemmelse, der også indebærer, at den primære begrænsning af bestemmelsens anvendelsesområde ligger i ”without authorization”. Da amerikanske domstoles afgørelser er langt mere udførlige i argumentationen for deres konklusioner, giver de i det mindste idéer – nogle gode og andre mindre gode – om hvordan man kunne fortolke bestemmelsen; fx hvilke faktiske omstændigheder har signaleret, at adgangen var ”without authorization” eller endda ”authorized”. Derudover skal både den amerikanske føderale hackerlovgivning og den danske hackerbestemmelse implementere

Europarådets cybercrimekonvention. På grund af de amerikanske domstoles større erfaring med cybercrime samt at USA, både på føderalt niveau og delstatsniveau havde haft hackerlovgivning i årevis, fik de amerikanske repræsentanter ved forhandlingerne og udarbejdelsen af konventionen angiveligt en særlig indflydelse. Dette følger både af de amerikanske myndigheders udtalelser, men det følger formentlig også naturligt af, at USA, på dette tidspunkt, utvivlsomt havde den største erfaring med emnet. Denne større amerikanske erfaring er også noteret i de danske forarbejder til hackerbestemmelsen, og er endvidere kommet til udtryk i Vagn Greves bog *edb-strafferet*, der udkom året efter hackerbestemmelsen blev vedtaget.

Afhandlingen analyserer derfor amerikansk føderal retspraksis med det til formål at få indblik i denne erfaring, som vores fælles konvention angiveligt er blev påvirket af og som gav anledning til bemærkninger i forarbejderne til den danske hackerbestemmelse. Formålet er at lære af denne erfaring – både det gode og det mindre gode – ikke med henblik på at overføre retsregler, da vi allerede har sammenlignelige bestemmelser, men for at finde frem til en analyseramme til brug ved anvendelsen af den meget bredt formulerede danske bestemmelse. Fordi begge bestemmelsers ordlyd er plaget af forholdsvis stor grad af uklarhed, så er det blevet domstolenes rolle, i begge lande, at frembringe en klarhed i anvendelsen. Denne retsanvendelse skal være tilstrækkelig forudsigelig og må ikke udgøre arbitrær retsanvendelse. Disse krav følger af den amerikanske forfatning og forfatningsretlige principper for de amerikanske domstoles vedkommende, og af artikel 7 EMRK og tilhørende principper udledt af EMD for de danske domstoles vedkommende. Derfor må den mulige analyseramme kunne leve op til disse krav om tilstrækkelig forudsigelighed og ikke-arbitrær retsanvendelse.

Resultatet af denne afhandling er derfor en analyseramme til brug for fortolkningen af ”uberettiget”, der ikke blot tager hensyn til den tekniske virkelighed og sociale normer, men som også er praktisk anvendelig for de danske domstole samt konventionskonform, i mangel af en ønskværdig nærmere præcisering af hackerbestemmelsens anvendelsesområde fra lovgivers side. Analyserammen fokuserer på udviklingen af sociale normer, men er i høj grad bygget på ”kode”, da det er kodens funktion, der i høj grad bestemmer hvorledes man opfatter de digitale omgivelser. Ved at ”patche” den amerikanske ”code-based approach” med sociale normer (inkluderet en slags berettiget forventning, som 1985-betænkningen lægger op til), opnås en analyseramme, der dels burde forhindre overinklusion af handlinger, der ikke har meget at gøre med de beskyttede interesser, og dels gør anvendelsen af hackerbestemmelsen mere konsekvent og forudsigelig, og dermed bliver det mindre sandsynligt, at arbitrære faktorer lægges til grund for domfældelse i sager hvor

handlingen nok er moralsk uacceptabel, men ikke klart er omfattet af bestemmelsen. Dette fordi risikoen for arbitrær håndhævelse stiger i takt med, at domstolene gives bred mulighed for skønsudøvelse ved uden at domstolene også har fået tilstrækkelig vejledning ift. hvad der faktisk ønskes kriminaliseret.

Inkluderet i afhandlingen, og i øvrigt i tråd med afhandlingens tema om uklarhed og IT-relaterede bestemmelser, er en artikel der omhandler straffelovens § 193. Straffelovens § 193 kriminaliserer den retsstridigt fremkaldte forstyrrelse i driften af nærmere angivne anlægstyper. Samtidig med at hackerbestemmelsen (straffelovens § 263, stk. 2) blev indført i 1985 indføjedes begrebet ”databehandlingsanlæg” (senere ændret til ”informationssystemer”) i opremsningen af de samfundsvigtige anlæg beskyttet af § 193. De andre anlæg, der er nævnt i bestemmelsen, har en meget mere specifik funktion, så som almene samfærdselsmidler og el-, gas- og vandværk, og er der er derfor sjældent tvivl om hvorvidt anlægget er objektivt omfattet af bestemmelsen. Hvorvidt en forstyrrelse af en af disse anlæg er ”omfattende” vil i så fald typisk være afhængigt af antallet af borgere, der påvirkes af forstyrrelsen. Der er ingen tvivl om, at begrebet ”informationssystemer” er utrolig bredt i mangel af nærmere afgrænsning, og at ikke alle informationssystemer har den samfundsvigtige karakter som bestemmelsen synes at forudsætte. I forarbejderne er den eneste vejledning til afgrænsningen af de for bestemmelsen relevante informationssystemer, at dette må være afhængigt af antal brugere. Denne afgrænsning af bestemmelsen er uden meget nytte, da mange informationssystemer har millioner af brugere uden at opfylde nogen som helst samfundsvigtig rolle, der tilnærmelsesvis er på højde med de andre samfundsvigtige systemer, som bestemmelsen nævner. Artiklen påpeger derfor, at der mangler en kvalitativ afgræsning, hvorefter man må foretage en kvalitativ vurdering af hvorvidt et givet informationssystem er samfundsvigtigt og derfor objektivt omfattet af bestemmelsen.

16 ABSTRACT IN ENGLISH

This year it has been thirty years since the Danish hacking provision was enacted. The drafters and the legislature were already at that time aware that the provision's language was capable of reaching conduct that was not meant to be criminalized. In order to rein in the very broad language the term "without right" was added. The term "without right" was meant to put the courts on notice regarding the fact that some conduct that fit the statutory language was legal nonetheless. The legislature meant for the courts to evaluate on a case-by-case basis whether the conduct was without right. The term "without right" is also used in other criminal law provisions on privacy violations for the same reason. It is of interest to gain understanding of how courts can or should exercise this rather broad discretion.

The provisions on privacy and dignity violations are generally very broadly phrased and their legal content does not follow clearly from the statutory language. The application of the other provisions, such as the criminal code § 264 on trespass onto another's property, is based on social norms that have been developing over the course of hundreds of years that then serve to clarify the provision and makes its application more or less foreseeable in the majority of cases. We know from experience and social norms that we cannot just enter a private residence, and we know that we must await an invitation to enter. But what constitutes a private residence, and thus when to expect the need to obtain a special permission to enter, is something we sense and deduce from the surroundings and circumstances; the statutory does not determine when a house is a private residence and thus does not determine when a special permission to enter is required or if there are circumstances where a special permission is not required nonetheless. It is not a violation of § 264 every time we enter another's property with special permission, because the environment and context may indicate other rules. For example when we go food shopping at a supermarket. Here we know that we do not need to obtain special permission to enter, even though the supermarket is the property of another. But, as mentioned, this does not follow from the statutory language, and Danish courts do not spend time explaining why this is the norm – perhaps because there is no need to when the norm is so widely known that it requires no explaining. However, with respect to interactions with computers to gain access to information and programs, the norms are still in their infancy and the courts are taking part in developing those norms, it is therefore rather important that courts explain why they perceive access to information and programs as being without right.

In 1985, when the hacking provision was enacted, there was no widespread experience with computers in society. In the mid-90s owning a computer had become more common, and combined with the advent of the web and more widespread availability of internet access the act of accessing information and programs belonging to others meant that the conduct the provision was capable of covering became more common. Especially the Internet and the world wide web, both of which directly involve accessing information and programs belonging to others, meant that "without right" become that much more important as a limiting factor on the hacking provision's application. Many questions arise regarding the interpretation of § 263(2) because we have not had that long a time to figure out what norms apply on the Internet or general with respect to computers; that is, when access is unauthorized and when it is authorized, whether a special permission is required and what circumstances indicate that an area is private or freely accessible without the need for special permission.

Even in cases involving employees and their access to their employers' computers and networks, which are the examples provided for in legislative history, it is still unclear what conduct constitutes a violation of the hacking provision. This uncertainty was already expressed in the 1985 Committee report, which proposed the provision.

Regrettably, there are few Danish court decisions regarding violations of § 263 (2), and the few that do exist are, with an exception or two, cases that are rather clearly a violation, or an attempted violation, of the hacking statute; for example, attempted access to another's computer using well-known hacking tools for the purposes of circumventing security measures. Compounding the problem related to understanding the scope of § 263(2) is the fact that Danish courts rarely provide detailed reasoning as to how they arrived at their conclusion. This frustrates an analysis of "why" and "how" a court arrived at any given decision, and makes it close to impossible to understand how they would apply the provision in other circumstances, because there are no hints as to their approach to interpreting and construing the provision other than the result of that process. This hinders foreseeability to a certain extent, which is problematic when the norms with respect to computers are not well-established, and the provision is capable of a very broad reach.

The courts have been delegated substantial discretion and there is little guidance to be found in legislative history. The courts are facing a tough assignment, which in 1985 was not particularly clear either even though computers were not a common household item and there was no widespread open access to information and programs belonging to others. Their task has not

become easier or better guided since the advent of the world wide web and massive interconnectivity made possible by the Internet, both of which are based on and serve the idea of information sharing. This means that courts must be careful in their application of the hacking statute, especially if it is not entirely clear whether access was with right.

Luckily, Denmark was not the only country that had enacted a broadly phrased hacking provision. The American federal courts have a few decades of experience with applying the federal hacking statute (the Computer Fraud and Abuse Act), which also heavily relies on a similar term, "without authorization", to delimit the scope of the hacking statute. The benefit of looking towards the US lies in the fact that US courts are by far more verbose and explicate their reasoning. This provides insights into how one could interpret the Danish hacking provision – whether the interpretations are desirable or not; for example, the courts often recount what may have signaled the presence or absence of authorization. Besides being ripe with interesting case law, the federal hacking statute also shares the fact with the Danish hacking provision that it implements the Convention on Cybercrime. Because the significant experience with cybercrime law in the US legal system, the US allegedly had significant influence on the drafting of the Convention. At least this is stated by the Department of Justice, but it does not seem like an unnatural or unreasonable suggestion given that the US was the first state in the world to enact hacking statutes, and thus, its experience was longer. This significant experience in the US is also noted in the legislative history of the Danish hacking provision, but also noted by one of the first Danish works on computer crime law, a book by Vagn Greve published the year after the hacking provision was enacted.

This dissertation analyzes US federal case law with a view to gaining an insight into US experiences, which to a greater or lesser degree influenced our common convention and which was noted in the Danish legislative history. The purpose of learning from US experience with hacking statutes – both good and bad experiences – is not to transfer legal rules, since we already have very similar hacking provisions. The purpose is to see what factual circumstances give rise to the application of the hacking statute and how the courts approach the discretion implicitly granted to them when the legislature used the words "without authorization". In other words, the interest is centered on deriving an analytical framework that avoids unforeseeable applications and arbitrariness. That criminal law must live up to requirements of clarity, including reasonable foreseeability (fair notice) and guarding against arbitrary enforcement of the law. This follows from the US Constitution and constitutional doctrines, and from article 7 ECHR and the ECtHR's article 7 case law. Any analytical framework would have to meet these requirements.

The dissertation discusses several approaches to interpreting and construing unauthorized access statutes in US law. The result of this dissertation is an analytical framework that can be used to interpret and construe "without right" in the Danish hacking provision. This framework takes into account the technical reality and social norms (developing and existing), and thus, contributes to foreseeability of the application of hacking statutes. The choice of framework is based on the results of analyses of the apparent inconsistencies and weaknesses of other approaches to construing unauthorized hacking statutes. This could perhaps in part make up for legislative inaction with respect to updating the very broad Danish hacking provision to provide more clarity and foreseeability of its application in a world that has changed significantly in terms of use of information technology since 1985.

Included in this dissertation is an article on the Danish criminal code § 193. The article follows the general underlying theme that is lack of clarity in technology-related criminal code provisions. The provision criminalizes the unlawful substantial interference with the operation of various systems that are best characterized as critical infrastructure. In 1985, "information systems" was added to the list of protected systems that until that point comprised e.g. water and power plants, public transportation, and the telephone network. Information systems can provide or support a long list of service, not all of which can be characterized as critical infrastructure. Thus, the article points out that not just any popular information system is protected by § 193, but that courts have to determine – not just through sheer number of users – whether the system performs a function that is considered critical for society, the interruption of which would be especially harmful, and thus calls for enhanced punishment.

17 BIBLIOGRAPHY

Cases

Denmark

- U 1979.188 V
- U 1981.679B
- U 1986.423/2Ø
- U 1987.216 Ø
- Dom afsagt af Retten i Roskilde 19.december 1996
- U 1996.979 Ø
- U 2000.261 Ø
- U 2001.1187 Ø
- U 2002.2700 V
- TfK 2003.160
- U 2005.1357 V
- TfK 2011.668
- U 2011.1144 Ø
- Case 146/2014 of 28 January 2015 where the Supreme Court cited and followed its own decision in UfR 1982.126

United States

- Marbury v. Marshall, 5 U.S. 137 (1803)
- Fletcher v. Peck, 10 U.S. 87 (1810)
- Cook v. United States, 288 U.S. 102, 120 (1933)
- Connally v. General Constr. Co., 269 U.S. 385, 46 S.CT. 126, 70 L.Ed. 888 (1939)
- Winters v. New York, 333 U.S. 507, 68 S.Ct. 665, 92 L.Ed. 840 (1948)
- Terry v. Ohio, 392 U.S. 1, 9, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968)
- Coates v. City of Cincinnati, 402 U.S. 611 (1971)
- Grayned v. City of Rockford, 408 U.S. 104, 108-109 (1972)
- Kolender v. Lawson, 461 U.S. 352 (1983)
- United States v. Morris, 928 F.2d 504 (2nd Cir. 1991)
- United States v. Sablan, 92 F.3d 865 (9th Cir. 1996)
- State v. Allen, 917 P.2d 848 (Kan. 1996)
- United States v. Czubinski, 106 F.3d 1069 (1st Cir. 1997)
- Reno v. American Civil Liberties Union, 521 U.S. 844, 870-871 (1997)

- America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444 (E.D. Vir. 1998)
- Muscarello v. United States, 524 U.S. 125, 138 (1998)
- Edge v. Professional Claims Bureau, Inc., 64 F.Supp.2d 115 (E.D. N.Y. 1999)
- Moulton v. VC3, 2000 WL 33310901 (N.D. Ga. 2000)
- Shaw v. Toshiba, 91 F.Supp.2d 942 (E.D. Texas 2000)
- Shurgard v. Safeguard, 119 F.Supp.2d 1121, 1125 (W.D.Wash. 2000)
- EF Cultural Travel v. Explorica, 274 F.3d 577, 580-581 (1st Cir. 2001)
- Fujitsu Ltd. v. Federal Exp. Corp., 247 F.3d 423 (2nd Cir. 2001)
- America Online v. National Health Care Discount, Inc., 121 F.Supp.2d 1255 (N.D. Iowa 2002)
- EF Cultural Travel v. Zefer Corp., 318 F.3d 58 (1st Cir 2003)
- Creative Computing v. Getloaded.com, 386 F.3d 930 (9th Cir. 2004)
- Hibbs v. Winn, 542 U.S. 88, 124 S.Ct. 2276 (2004)
- Register.com v. Verio, 356 F.3d 393 (2nd Cir. 2004)
- Southwest Airlines v. Farechase, 318 F.Supp.2d 435 (N.D. Tex. 2004)
- Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004)
- International Association of Machinists and Aerospace Workers v. Werner-Masuda, 390 F.Supp.2d 479 (D. Md. 2005)
- International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006)
- Lockheed Martin v. Speed, 2006 WL 2683058 (M.D. Fla. 2006)
- ViChip v. Lee, 438 F.Supp.2d 1087 (N.D. Cal. 2006)
- Diamond Power International v. Davidson, 540 F.Supp.2d 1322 (N.D. Ga. 2007)
- Healthcare Advocates v. Harding, 497 F. Supp. 2d. 627 (E.D. Pa. 2007)
- Southwest Airlines v. Boardfirst, 2007 WL 4823761 (N.D.Tex. 2007)
- Ticketmaster LLC v. RMG Technologies, 507 F.Supp.2d 1096 (C.D. Cal. 2007)
- United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007)
- United States v. Willis, 476 F.3d 1121 (10th Cir. 2007)
- Medellín v. Texas, 128 S. Ct. 1346, 1357, 552 U.S. 491 (2008)
- Shamrock Foods Company v. Gast, 535 F.Supp.2d 962 (2008)
- United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)
- LVRC Holdings v. Brekka, 581 F.3d 1127 (9th Cir. 2009)
- Cvent v. Eventbrite, 739 F.Supp.2d 927 (E.D. Vir, 2010)
- Orbit One Communications v. Numerex, 692 F.Supp.2d 373 (S.D.N.Y. 2010)
- United States v. John, 597 F.3d 263 (5th Cir. 2010)
- United States v. Lowson, 2010 WL 9552416 (D.N.J. 2010)
- United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)
- Koch Industries v. Does, 2011 WL 1775765 (D. Utah 2011)
- Lee v. PMSI, 2011 WL 1742028 (M.D. Fla. 2011)
- Pulte Homes v. LIUNA, 648 F.3d 295 (6th Cir. 2011)
- United States v. Teague, 646 F.3d 1119 (8th Cir. 2011)
- FCC v. Fox Television Stations, Inc., 567 U.S. XXX (2012)

- United States v. Nosal, 676 F.3d 854 (9th Cir. (en banc) 2012)
- WEC Carolina Energy Solutions, LLC v. Miller, 687 F.3d 199 (4th Cir. 2012)
- Craigslist v. 3Taps, 2013 WL 4447520 (N.D. Cal. 2013)
- Dresser-Rand Company v. Jones, 2013 WL 3810859 (E.D. Pa. 2013)
- US v. Auernheimer, 2014 WL 1395670 (C.A.3 (N.J.))
- United States v. Steele, 595 Fed.Appx. 208 (4th Cir. 2014)
- United States v. Shen, 2015 WL 3417471 (E.D. Missouri 2015)
- United States v. Valle, 301 F.R.D. 53 (S.D.N.Y. 2014)

Sweden

- Svea Hovrätt RH 2015:15
- NJA 2014 s. 221 (NJA 2014:19)

ECtHR

- Golder v. United Kingdom, Judgment of 21 January 1975
- Kokkinakis v. Greece, Judgment of 25 May 1993
- C.R. v. United Kingdom, Judgment of 22 November 1995
- H.M.A. v. Spain, Application no. 25399/94, Decision of 9 April 1996 on the admissibility of the application
- Cantoni v. France, Judgment of 11 November 1996
- Başkaya and Okçuoglu v. Turkey, Judgment of 8 July 1999
- Coeme & Others v. Belgium, Judgment of 22 June 2000
- N.F. v. Italy, Judgment of 2 August 2001
- Achour v. France, Judgment of 29 March 2006
- Pessino v. France, Judgment of 10 October 2006
- Custers, Deveaux and Turk v. Denmark, Judgment of 3 May 2007
- Kafkaris v. Cyprus, Judgment of 12 February 2008
- Liivik v. Estonia, Judgment of 25 June 2009
- Camilleri v. Malta, Judgment of 22 January 2013
- Ashlarba v. Georgia, Judgment of 15 July 2014

CJEU (formerly ECJ) and AG opinions

- Case 26/62 Van Gend en Loos
- Case 6/64 Costa v. ENEL

- Case 14/83 Von Colson v. Land Nordrhein-Westfalen
- C-80/86 Kolpinghuis Nijmegen
- Joined cases C-74/95 and C-129/95 X
- C-105/03 Pupino
- C-176/03 Commission v. Council

- Opinion of Advocate General Colomer in Joined Cases C-74/95 and C-129/95 X
- Opinion of Advocate General Kokott in C-105/03 Pupino

Literature

- Mads Bryde Andersen: EDB og Ansvar (1988), Jurist- og Økonomforbundets Forlag
- Mads Bryde Andersen: Lærebog i EDB-RET (1991), 1st edition, Jurist- og Økonomiforbundets Forlag
- Mads Bryde Andersen: IT-retten (2005), 2nd edition, Gjellerup
- Mads Bryde Andersen and Joseph Lookofsky: Lærebog i obligationsret I – Ydelsen Beføjelser (2010), 3rd edition, Thomson Reuters
- Kristina Ash: U.S. Reservations to the International Covenant on Civil and Political Rights: Credibility Maximization and Global Influence (2005), 3 Nw. Univ. J. Hum. Rts. 1
- Andrew Ashworth and Jeremy Horder: Principles of Criminal Law (2013), 7th edition, Oxford University Press
- Patricia L. Bellia: Defending Cyberproperty (2004), New York University Law Review, Volume 79, p. 2164. Available at http://ssrn.com/abstract=714243
- Randy E. Barnett: Interpretation and Construction (2011)
- Robert Batey: Vagueness and the Construction of Criminal Statutes – Balancing Acts (1997), 5 Va. J. Soc. Pol'y & L. 1
- Trine Baumbach: Det strafferetlige legalitetsprincip (2008), 1st edition, Jurist- og Økonomforbundets Forlag
- Trine Baumbach: Strafferet og menneskeret (2014), 1st edition, Karnov Group
- Matt Bishop: Position: "Insider" is Relative (2006). Available at http://www.nspw.org/papers/2005/nspw2005-bishop-pos.pdf
- Matt Bishop and Carrie Gates: Defining the Insider Threat (2008). Available at https://web.cs.dal.ca/~gates/papers/csiirw08.pdf
- Susan W. Brenner: Cybercrime and the Law: Challenges, Issues, and Outcomes (2012), Northwestern University Press
- Dan L. Burk: The Trouble with Trespass (2000). Available at http://ssrn.com/abstract=223513
- Bent Carlsen and Michael Elmer: Datakriminalitet (1986), Juristen

- Malene Bechmann Christensen: Det strafferetlige samtykke (2008), 1st edition, Jurist- og Økonomforbundets Forlag
- Jonathan Clough: Principles of Cybercrime (2010), 3rd printing, Cambridge University Press
- Katherine Clark and Matthew Connolly: A Guide to Reading, Interpreting and Applying Statutes (2006), The Writing Center at Georgetown University Law Center
- Congressional Research Service Annotated Constitution: Tenth Amendment. Available at Cornell's website at https://www.law.cornell.edu/anncon/html/amdt10_user.html#amdt10_hd7. Last visited on 31 August 2015
- Congressional Research Service Annotated Constitution, p. 1747 (Due Process, Fourteenth Amendment). Available at http://www.law.cornell.edu/anncon/html/amdt14efrag2_user.html. Last accessed on 21 February 2015.
- Evan J. Criddle: The Vienna Convention on The Law of Treaties in U.S. Treaty Interpretation (2004), Virginia Journal of International Law 44
- John F. Decker: Addressing Vagueness, Ambiguity, and Other Uncertainty in American Criminal Laws (2002), 80 Denv. U. L. Rev. 241
- Audra D. Dial and John M. Moye: The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers From Trade Secret Theft? (2013), 64 Hastings L.J. 1447
- William N. Eskridge: Dynamic Statutory Interpretation (1987), University of Pennsylvania Law Review, Volume 135, No. 6, pp. 1479-1555
- E. Allan Farnsworth: An Introduction to the Legal System of the United States (2010), 4th edition (edited by Steve Sheppard), Oxford University Press
- Katherine Mesenbring Field: Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act (2009), 107 Mich. L. Rev. 819
- P. Freitas and N. Gonçalves: Illegal access to information systems and the Directive 2013/40/EU (2015), International Review of Law, Computers & Technology, Volume 29 Issue 1, pp. 50-62
- Christine D. Galbraith, 'Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites' (2004), 63 Md. L. Rev. 320
- Michael John Garcia (Congressional Research Service): International Law and Agreements: Their Effect upon U.S. Law (23 January 2014)
- Marco Gercke: Understanding Cybercrime: Phenomena, Challenges and Legal Response (2012), p. 182. Available at http://www.itu.int/INT-D/cyb/cybersecurity/legislation.html
- Peter Germer: Statsforfatningsret (2007), 4th edition, 3rd printing, Jurist- og Økonomforbundets Forlag
- Stephanie Greene and Christine Neylon O'Brien: Exceeding Authorized Access in the Workplace: Prosecuting Disloyal Conduct Under the Computer Fraud and Abuse Act (2013), 50 Am. Bus. L.J. 281
- Vagn Greve: edb-strafferet (1986), 2nd revised edition, Jurist- og Økonomforbundets Forlag
- Carsten Munk-Hansen: Retsvidenskabsteori (2014), 1st edition, Jurist- og Økonomforbundets Forlag

- Oona A. Hathaway, Sara Aronchick Solow and Sabria McElroy: International Law at Home: Enforcing Treaties in U.S. Courts (2012), Yale Journal of International Law, Volume 37, No. 1, p. 51
- Pieter Hintjens: Culture & Empire (2013), 1st edition, iMatix Global Services
- Jeffrey Hunker and Christian W. Probst: Insiders and Insider Threats: An Overview of Definitions and Mitigation Techniques (2008), Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 2, No. 1
- IETF: RFC 2616, Abstract. Available at http://www.rfc-base.org/txt/rfc-2616.txt. Last visited on 10 July 2015.
- Jacobs, White, & Ovey: The European Convention on Human Rights (2010), 5th edition, Oxford University Press
- John Calvin Jeffries, Jr.: Legality, Vagueness, and the Construction of Penal Statutes (1985), Virginia Law Review, Vol. 71, No. 2, pp. 189-245
- Malene Frese Jensen, Vagn Greve, Gitte Høyer & Martin Spencer: The Principal Danish Criminal Acts (2006)
- Justitsministeriet: Vejledning om lovkvalitet (2005)
- Matthew Kapitanyan: Beyond WarGames: How the Computer Fraud and Abuse Act Should be Interpreted in the Employment Context (2012), 7 I/S: J. L. & Pol'y for Info. Soc'y 405
- Orin S. Kerr: The Problem of Perspective in Internet Law (2003), Georgetown Law Journal, Vol. 91, pp. 357-405. Available at http://ssrn.com/abstract_id=310020
- Orin Kerr: Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes (2003), NYU Law Review, Vol. 78, No. 5, pp. 1596-1668. Available at http://ssrn.com/abstract=399740
- Orin S. Kerr: Vagueness Challenges to the Computer Fraud and Abuse Act (2010), 94 Minnesota Law Review 1561. Available at http://ssrn.com/abstract=1527187
- Orin S. Kerr: Norms of Computer Trespass (May 2015 draft), Columbia Law Review (Forthcoming 2016), p. 5. Available at: http://ssrn.com/abstract=2601707
- Jon Fridrik Kjølbro: Den Europæiske Menneskerettighedskonvention – for praktikere (2010)
- Wayne R. LaFave: Criminal Law (2010)
- Lars Bo Langsted, Peter Garde and Vagn Greve: Criminal Law Denmark (2014)
- Joseph Lookofsky: Precedent and the Law in Denmark (2006), Danish National Report, XVIIth Conference of the International Academy of Comparative Law
- Nancy E. Marion: The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation (2010), International Journal of Cyber Criminology, Volume 4, Issue 1 & 2
- David McGowan: Website Access: The Case for Consent (2003), 35 Loy. U. Chi. L. J. 341, Volume 35, Issue 1
- Cian Murphy: The Principle of Legality in Criminal Law under the ECHR (2010), European Human Rights Law Review, Vol. 2, p. 9. Available at http://ssrn.com/abstract=1513623.
- Ulla Neergaard and Ruth Nielsen: EU ret (2010), 6th revised edition, Thomson Reuters
- Ruth Nielsen and Christina D. Tvarnø: Retskilder & Retsteorier (2005), 1st edition, Jurist- og Økonomforbundets Forlag

- Note, The New Rule of Lenity (2006), 119 Harvard Law Review 2420
- Pfleeger, Predd, Hunker and Bulford: Insiders Behaving Badly: Addressing Bad Actors and Their Actions (2010), IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1
- Charles P. Pfleeger: Computer Security, AccessScience. McGraw-Hill Education, 2014
- Lorenzo Picotti and Ivan Salvadori: National legislation implementing the Convention on Cybercrime – Comparative analysis and good practices (2008). Available on the Council of Europe's website at https://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20study2-d-version8%20_28%20august%2008.pdf
- Zachary Price: The Rule of Lenity as a Rule of Structure (2004), 72 Fordham L. Rev. 885, Volume 72 Issue 4
- Max Radin: Statutory Interpretation (1930), Harvard Law Review, Vol. 43, No. 6
- Mathias Reimann and Richard Zimmerman: Oxford Handbook of Comparative Law, Markus Dirk Dubber: Comparative Criminal Law (2008), 1st edition, Oxford University Press
- Rigsadvokatens meddelelse nr. 9/2005
- Alf Ross: Om ret og retfærdighed (2013)
- Bjørn Saltorp and Erik Werlauff: Kontrakter (2009), 2nd edition, Jurist- og Økonomforbundets Forlag
- Russell G. Smith, Peter Grabosky and Gregor Urbas: Cyber Criminals on Trial (2004), Cambridge University Press
- Lawrence B. Solum: The Interpretation-Construction Distinction (2010), 27 Constitutional Commentary 95-118
- Ole Spiermann: Moderne folkeret (2006), 3rd edition, Jurist- og Økonomforbundets Forlag
- Josephine Steiner and Lorna Woods: EU Law (2009)
- Sarah Summers: EU Criminal Law and the Regulation of Information and Communication Technology (2015)
- Karsten Engsig Sørensen and Poul Runge Nielsen: EU-retten (2010), 5th edition, Jurist- og Økonomforbundets Forlag
- Warren Thomas: Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act (2010), Georgia State University Law Review, Volume 27, Issue 2, Article 14. Available at http://readingroom.law.gsu.edu/gsulr/vol27/iss2/14
- Takis Tridimas: The General Principles of EU Law (2006), 2nd edition, Oxford EC Law Library
- Jan Trzaskowski (ed.): Internetretten (2012), 2nd edition, Ex Tuto Publishing
- Henrik Udsen: De informationsretlige grundsætninger – Studier i informationsretten (2009), 1st edition, Jurist- og Økonomforbundets Forlag
- UNODC Comprehensive Study on Cybercrime – February 2013
- Michael A. Vatis: The Council of Europe Convention on Cybercrime (2010), Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy. Available at http://cs.brown.edu/courses/csci1950-p/sources/lec16/Vatis.pdf

- Jørn Vestergaard & Flemming Balvig (ed.): ›› Med lov…‹‹ Retsvidenskabelige betragtninger (1998), Mads Bryde Andersen: Overvågning af medarbejderne, Jurist- og Økonomforbundets Forlag
- Knud Waaben and Lars Bo Langsted: Strafferettens almindelige del I – Ansvarslæren (2011), 5th edition, 2nd printing (2012), Karnov Group
- Ian Walden: Computer Crimes and Digital Investigations (2007), 1st edition, Oxford University Press
- Morten Wegener: Juridisk metode (2000), 3rd revised edition, Jurist- og Økonomforbundets Forlag
- Peter A. Winn: The Guilty Eye: Unauthorized Access, Trespass and Privacy (2007), 62 Bus. Law. 1395

ISSN (online): 2246-1256
ISBN (online): 978-87-7112-839-0

AALBORG UNIVERSITY PRESS