Privacy for Sale?

Analysis of Online User Privacy

Sørensen, Lene Tolstrup; Sørensen, Jannick Kirk; Khajuria, Samant

Publication date:
2015

CMI working paper no. 8, 2015

Privacy for Sale? – Analysis of Online User Privacy

Lene Sørensen, Jannick Kirk Sørensen
and Samant Khajuria

Center for Communication, Media and
Information technologies (CMI), Electronic
Systems, AAU Copenhagen, Denmark

CMI Working Paper no. 8:

Lene Sørensen, Jannick Kirk Sørensen and Samant Khajuria (2015) *Privacy for Sale? – Analysis of Online User Privacy*. AAU, Copenhagen

ISBN: 978-87-7152-079-8

Published by:
center for Communication, Media and Information technologies (CMI)
Department of Electronic Systems,
Aalborg University Copenhagen,
A.C. Meyers Vænge 15,
DK-2450 Copenhagen SV
Tel +45 99403661
E-mail cmi@cmi.aau.dk
URL http://www.cmi.aau.dk

CMI Working Papers provide a means of early dissemination of completed research, summaries of the current state of knowledge in an area, or analyses of timely issues of public policy. They provide a basis for discussion and debate after research is completed, but generally before it is published in the professional literature.

CMI Papers are authored by CMI researchers, visitors and participants in CMI conferences, workshops and seminars, as well as colleagues working with CMI in its international network. Papers are refereed before publication. For additional information, contact the editors.

Editor: Anders Henten, co-editor: Jannick Sørensen

Privacy for Sale?

– Analysis of Online User Privacy

Lene Sørensen, Jannick Kirk Sørensen and Samant Khajuria

Center for Communication, Media and Information Technologies (CMI), Department of Electronic Systems, Aalborg University, Copenhagen, Denmark
(ls@cmi.aau.dk; js@cmi.aau.dk; skh@cmi.aau.dk)

Abstract. Data brokers have become central players in the collection online of private user data. Data brokers' activities are however not very transparent or even known by users. Many users regard privacy a central element when they use online services. Based on 12 short interviews with users, this paper analyses how users perceive the concept of online privacy in respect to data brokers collection of private data, and particularly novel services that offer users the possibility to sell their private data. Two groups of users are identified: Those who are considering selling their data under specific conditions, and those who reject the idea completely. Based on the literature we identify two positions to privacy either as an instrumental good, or as an intrinsic good. The paper positions various user perceptions on privacy that are relevant for future service development.

Keywords: User privacy; informational privacy; privacy negotiations; data brokers.

1 Introduction

Managing and understanding personal privacy is for many online users becoming a key issue with the increasing use of Internet services. Numerous incidents and problems are portrayed in the media on hacking, misuse, tracking, and overstepping private privacy of users [12], [29]. Studies show that users generally are becoming more aware of privacy problems online and that most users do think and do something in order to manage their privacy [1].

One of the central elements in online user privacy is the upcoming of the so-called data brokers [7]. Data brokers are defined as: "*companies whose primary business is collecting personal information about consumers from a variety of sources and aggregating, analysing, and sharing that information, or information derived from it, for purposes such as marketing products, verifying an individual's identity, or detecting fraud*" [7]. Data brokers do not have any direct contact with users but collect and buy private data from online services – government institutions, mobile apps, web sites etc. Many people are unaware of the data brokers and their activities [7], [8].

As a result of the raise in privacy concerns as well as in data brokers, there is a growth in new services that bring the private users into the market place for private data. One example is the service Datacoup (datacoup.com) that offer private users 8$ a month for insights on their private data produced on social media and credit and debit cards [27]. Additionally, there exist a number of visualization tools that can offer the user visual aid in understanding where (in which services) the data brokers have access to information (see an overview in [16]).

The purpose of this paper is to analyse the concept of user privacy and the perspective of bargaining where users can control their private data by engaging in an economic relation with service providers or data brokers on private data. The paper is based on 12 short interviews asking users about their perception of online privacy and the idea of a data market. The interviews are analysed using a conceptual framework of intrinsic versus instrumental privacy [20].

The organisation of the paper is as follows: Section 2, the concept of user privacy is presented from a literature point of view. Section 3 presents some of the characteristics and issues raised with data brokers in the commercial handling of user privacy. In section 4, the empirical study is presented in terms of set-up, results of interviews as well as analysis. Section 5 discusses the findings of the interviews and finally, section 6 presents the presentation.

2 User Privacy

Historically, the term 'privacy' dates back to 1890 [33] and it was phrased as 'the right to be let alone' – in terms of individuals' right to control how their personal attributes like a photo or voice is used in the public. This 'right of publicity' [24] perspective has – besides its financial aspects described by later authors [10], - also gained importance today through social media since it is highly relevant for what the sociologist Erving Goffman in 1956 introduced as "The Presentation of Self in Everyday Life" [11] – namely our desire to control how we are perceived by others, cf. [14], [31]. Today it is however often the terms 'informational privacy' and 'user privacy' which are discussed both in the policy and regulation literature, the HCI literature and in an large number of solution-oriented technical papers.

The philosopher James Moor [20], writing in the shift from a paper-based society to a digitized, discusses why the monitoring of his shopping habits, the pizza-baker's knowledge of his pizza preferences and the availability of his phone number on the world wide web feels like a privacy breach although they are not in classic sense. He suggests, *"[w]hen information is computerized, it is greased to slide easily and quickly to many ports of call. This makes information retrieval quick and convenient. But legitimate concerns about privacy arise when this speed and convenience lead to the improper exposure of information. Greased information is information that moves like lightning and is hard to hold onto."* [20:p. 27]

Throughout the article, he juxtaposes information remembered and used by a human with information stored and processed by computers, e.g.: "*Computers have elephant*

memories - big, accurate, and long term. The ability of computers to remember so well for so long undercuts a human frailty that assists privacy. We, humans, forget most things" [20:27]. Moor's central objection is however the collection of information now powered by computers: that "*information is collected and transmitted without any of us giving it a second thought*", and since it is "*greased*" it is "*ready to go for* any *purpose*" [20:28, original emphasis].

To analyse privacy in this context, he suggests with help from philosophy to discern between instrumental goods and intrinsic goods. Instrumental goods are used to obtain something else, like a bicycle that I can use for transportation. An intrinsic good is something that is good in it self, e.g. joy. In the literature he finds examples of privacy described as an instrumental good, e.g. that privacy protect us against harm (p. 28), but one can think of other ways to protect oneself against harm. The 'instrumental good' is thus not a very strong argument for something, since you can find alternative solutions. Moor [20:28] finds also examples of privacy depicted as an intrinsic good, e.g. in [15]: Privacy is as an essential aspect of autonomy. But this argument can also be countered by a thought experiment of a couple living together in complete transparency without hiding anything. To overcome these two weak arguments for privacy, he suggests that privacy is essential for the societal core value security, since *"[p]rivacy does enable us to form intimate bonds with other people that might be difficult to maintain in public*" [15:28]. Privacy is thus necessary for the functioning and flourishing of larger societies, Moor argues. This argument points more the debate away from 'user privacy', since this concept primarily look at the individual, and more in direction of the principles of 'informational privacy'.

The distinction between the two individual-oriented concepts of privacy as instrumental or intrinsic, and the collective approach in privacy as prerequisite for societal stability and growth is productive both when research literature and empirical data, like interviews with users, is analysed. An example of the instrumental approach is Thompson [30] who suggests a 'risk-based approach' to privacy. Analytically, he suggests to ask: 1) "*What is the probability that an excluded party will acquire the information?*", 2) "*What is the likelihood that harm will befall the affected party if the information is acquired by an excluded party?*" and 3) "*How serious is the harm that might befall the affected party?*" (ibid. p. 16-17). This approach, Thomson argues, helps identifying "*what is ethically important, as well as what is ethically problematic*" (ibid. p. 13). An example of the intrinsic approach could be Brey, [5], who worries of humans' loss of autonomy to machines in the context of a smart home / Ambient Intelligence. An example of the core value approach could be Vedder, [32], who argues against the possible de-individualisation when computer systems judge in a single case (e.g. whether one can get a loan) based on collective data, statistics or one's properties. In the analysis we will return to the three different arguments for privacy.

3 Data Brokers

Today personal data is an economic asset, unfortunately not to its rightful owner i.e., the user but to interested parties whose business case often revolves around user's data. These so-called interested parties are commonly known as 3rd parties used for tracking, analysing and storing user data. These parties are not necessarily problematic; many services rely on user data to provide relevant content and enhance user experience. For a couple of decades, much of this used to be data marketing strategies (customer relations management). What has changed is the volume and the nature of the data being mined from the Internet and user mobile devices by the multi-billion Euro industry that operate in the shadows with virtually no oversight.

Over the past couple of years a huge amount of attention is paid over the government organizations like the National Security Agency (NSA) snooping, bulk collection and storage of vast amount of raw data under the programs like PRISM all in the name of national security [19].

What users don't know or not aware of is the much greater and more immediate threat to the privacy coming from the thousands of companies that users have never heard about in the name of commerce, known as "Data Brokers" [7]. The companies are collecting, analysing and packaging some of users' most sensitive personal information and selling it as a commodity to each other, advertising companies and even government organizations often without users' direct knowledge. Everyday users involve themselves in multiple online and offline activities like playing games on mobile devices, using maps, online shopping, browsing, social media, internet surveys for discounts etc. In all these activities users reveal some personal information about them and the parties' they interact with and this may be collected as information and sold to data brokers. This is illustrated in Figure 1.

A number of privacy aware tools are developed in the form of browser add-on's and mobile apps to make users aware about their online data privacy. These tools enable the user to see the sites the user is interacting with knowing and unknowingly i.e., first and third party sites respectively. In addition to that some of these tools are also capable of detecting and stopping third-party trackers from secretly tracking users.

The following tools are representative for services that exist now and they provide an insight to the variety of existing privacy aware tools. The tools are broadly categorized into privacy aware-browser extensions and privacy protection-browser extension and mobile apps to illustrate the difference in privacy support these tools may provide to the user.

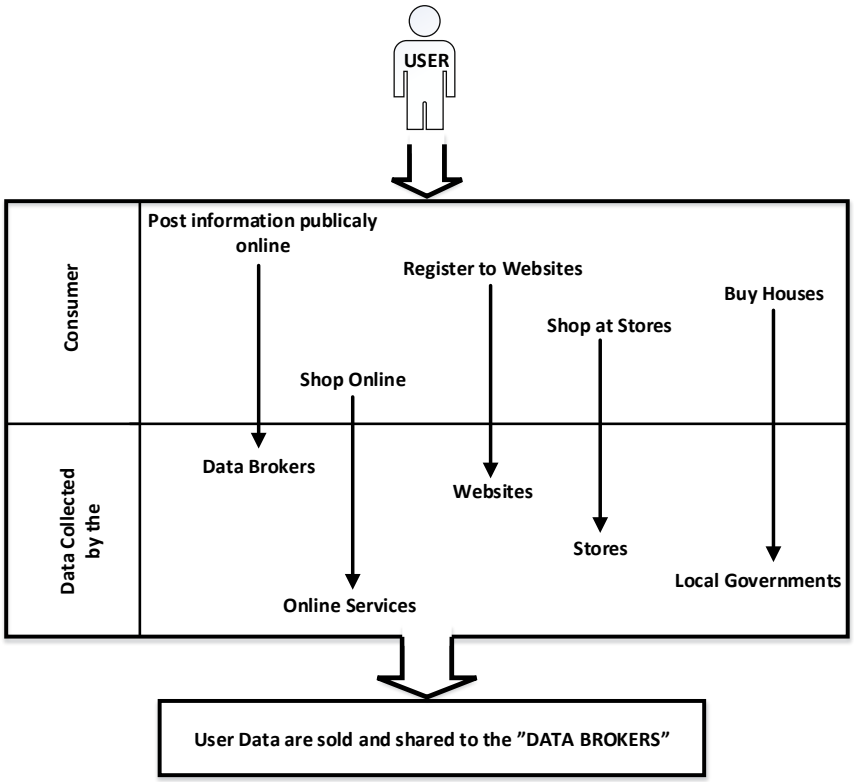

Fig. 1. The data flow between private users and Data Brokers

Tools working as Privacy Aware-Browser Extensions

The LightBeam [21] tool is a browser plugin developed by Mozilla that enables graphical representation of the first and third party sites interacting with the browser, revealing the full depth of the Web today, including parts that are not transparent to the average user. Using three distinct interactive graphic representations (Graph, Clock and List) it provides insights of individual third parties over time and space, and allows users to identify where they connect to their online activity. The graph gives a real time visualization of all third party requests in the moment a user visit a specific website. The clock allows for examining connections over a 24 hours period. And the list view enables the user to block sites from connecting with the Firefox browser. The user has the possibility to set up filters to see more types of data. The LightBeam tool uses lists and plots over the data information.

Well known to most online users, the Terms of Service text is the first step to privacy awareness. In most the cases, the Terms of service text is often too long to read and the users simply accept the terms without reading it. However it important to under-

stand what is in the Terms of Service and that the rights of the user depends on them. The service called “Terms of Service; Didn’t read” [29] is a browser extension that rate and analyse Terms of service and Privacy policies in order to create a rating from class A to class E. Terms of service are reviewed by legal experts and divided into small points that can be discussed, compared and ultimately.

Tools working as Privacy Protection-Browser extensions and Mobile apps

Privacy Badger [6] is a plug-in build on a tracker protection approach for browsers developed by the Electronic Frontier Foundation (EFF). The purpose is to analyse and block trackers or ads that violate the user consent. The extension is designed to automatically protect user privacy from third party trackers by letting the user block trackers that may be surreptitiously keeping track of the user's web activity. It can function without any setting, knowledge or configuration by the user and is therefore relatively easy to use for anyone. A so-called third party tracker (trackers which track browsing habits in order to display customized ads) is key in this tool. The user is presented with a slider in the Privacy Badger menu that shows a green, yellow or red dependent on level of tracking from different third parties.

The F-secure Freedome [23] is a VPN service that keeps the user invisible for anonymous browsing by masking the IP address under the protective cloud. Additionally, the app also gives the user a possibility of safe browsing and being un-trackable by scanning for malwares and blocking 3rd party / data brokers. The app has an interface with a large button in the middle that shows whether the user is protected or not. The features are provided against a monthly fee.

F-Secure App permissions [23] is another application that displays the permission of the apps installed on an Android device. It categorizes and ranks the apps based on the permissions it requests. It also informs about the ramifications of the given permissions. App Permissions analyses only apps that have already been installed.

Recently AVG has also developed an online privacy dashboard. AVG PrivacyFix [2] is a browser add-on and mobile app for privacy issues based on a user’s Facebook, Google and Linkedin settings. The dashboard gives a user visual representation of what personal data one has exposed and gets advice on how to fix it. The PrivacyFix also lets user know what their data is worth (economically) for example to Facebook and Google.

Another privacy-aware tool for the protection of users’ personal online information is MyPermissions [22] – it creates an online privacy shield by Online Permissions Technologies for browsers and applications on Android and Apple devices. The application offers an interface, so the user is able to manage all services permissions in one screen. The app provides information about the permissions requested by other apps like – if an app is acting on the user’s behalf, knows the user’s location, can access inbox or contact information, and basic permissions, e.g., posting on social media websites on the user’s behalf. The app gives users the possibility to Revoke, Trust or Report the permissions requested by other apps. Additionally, the MyPermissions app keep track of other apps’ updates, where they might ask for more infor-

mation about the user's personal data than originally granted, when the app was first installed.

These services are examples of different ways that users can control and manage the interest from data brokers – aspects that will be discussed more in the following empirical analysis.

4 The Interviews

Twelve short interviews have been carried out to provide insight into user privacy and the perspective or controlling data and engaging in privacy bargains.

4.1 The Set-Up

The interviews were carried out using a non-probabilistic, convenience sampling approach [17]. The perspective of online privacy is central to all users of online activities and in Denmark the penetration rate of online services is so high it is more probable to meet someone who is active online than meeting a person who is not. It was decided to recruit respondents on the university campus by conveniently, and randomly approaching persons sitting alone working anywhere on campus (for example in the cantina, in the hall way, in special areas for group work). Using convenience sampling at the university gave possibilities for the interviewer to take rounds at the university premises several times during various days, and to sit in friendly, well-known premises during the interviews.

The reason for targeting persons sitting alone was to raise the probability of an interview (it is more easy to talk to one person than to take a person away from a group), and to be able also to approach non-students at the university (workers, professors, etc.). The interviewer of course did try to avoid known university affiliates.

A total of 12 short interviews were carried out – with 7 female and 5 male respondents. Using the method presented in [13] it was seen that 12 interviews would be sufficient to get a sort of saturation on the interview questions. Short interviews (between 6-10) minutes were used. Short interviews (see [28]) has the advantage that respondents often can spare this time and are more inclined to take part in the interview and the short time is sufficient to create insight into the questions.

All recruited respondents were interviewed using a semi-structured interview guide with open questions [18]. Sub-questions were asked if the respondent's response did not cover the question completely. The guide consisted of 16 questions which was divided into the following sections:

- Questions on age and habit in terms of use of online services
- Questions on habit in terms of privacy management and definition of user privacy online

- Questions on direct feedback to variations of privacy services and situations in which they would act directly as entity in a privacy bargain and engaging in selling private data to data brokers.

The full interview guide can be found in the Annex.

Data were collected during two days in December, 2014. Interviews were conducted in either English or Danish dependent on the preferences from the respondent. Since the respondents were recruited by coincidence, there was no way of knowing whether it was an international or Danish person. The interview guide was in English for convenience of the interviewer. All interviews were tape recorded and later summarised and partly transcribed. One of the authors of this paper performed all interviews to secure consistency in terms of questions and how they were presented.

The distribution of respondents in terms of gender, age and language for the interview can be seen in Table 1.

Table 1. Overview of respondents' gender, age and language used for interviews

Person	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***	***12***
Gender	F	M	M	M	M	F	F	F	F	F	F	M
Age	24	32	28	23	29	25	35	23	23	25	23	26
Language	En	D	En	D	En	En	D	D	D	D	D	D

F= Female, M=Male, En – English language, D – Danish language

It shall be mentioned that the respondents 8-12 were in a group when interviewed. One of the persons in the group was approached (sitting alone), however everybody in the group (sitting not so far away so they could see it) were interested in participating and therefore, they suggested doing a common interview. The interviewer, however, made sure to get answers from all respondents in the group.

4.2 Results and Analysis

In the following the results of the interviews will be presented and analysed based on the framework presented in Section 2. This framework discerns, based on Moor, [20], between the user perceptions of privacy as an instrumental or intrinsic value. Within the instrumental/intrinsic distinction, we see specific privacy concerns that can be related to the literature presented in Section 2. In line with [11], [14], [31] and [33] a number of respondents express the need to control how they are appearing in different media. Another aspect, raised by the respondents, is asymmetrical distribution of information – that the collector of the data (here the data broker) does more about you than you know about the firm. This, together with the feeling that the system 'knows you' is aligned with the issue that Moor raises. Finally, if personal data is to be sold to

data brokers some respondents questions the transparency and fairness of this trade; are data brokers trustworthy trade partners?

In the following we will apply this framework on the interviews, represented by characteristic quotations. The numbering of the questions corresponds to the interview guide numbering in Annex.

In the interview, the respondents were first asked about their experience in terms of use of online services (questions 3 and 4). Generally the respondents were using online services (for student work, social media, gaming, browsing etc.) between 5 and 10 hours every day. It was not something that the respondents were clear on but was estimated during the interview. All together, the answers indicate that all respondents were daily users of several Internet services.

The respondents were asked if "*they take action to protect privacy while using the Internet – and why/why not*" (question 5). Generally, the respondents are aware of privacy and set privacy settings on Facebook, some look for spyware, but none of the respondents thought they did enough. This can be seen in the following citations:

> "*I think about privacy – but also think I am a bit ignorant*" (Person 1)
>
> "*Yes I do take care of my social media profile*" (Person 5)
>
> "*No I do not think I do enough*" (Person 8)

None of the respondents mention that they think about or do something about data brokers generally.

When it came to defining what "*the word privacy means for the respondent*" (question 9a), the answers fell into almost the same direction however with some details. Most of the respondents focus on being in control of the data and making sure that they can determine who to share data with. That can be seen from this comment:

> "*It means that I am in control over which data or information other can see about me. I should have control of everything*". (Person 4)
>
> "*I think it is irritating that others uploads something about me – I would have liked to place it there myself so I can control it. You can get a notification so you will be able to approve a picture others uploads – but it will still be on her profile (referring to Facebook)*". (Person 8)

These statements point at the Goffman "Presentation of Self" [11] rationale; privacy serves the purpose of helping controlling how one is perceived. It also echoes Johnson's [15] argument that privacy is an essential aspect of autonomy. Respondents have however clear ideas of how they want to present themselves at different platforms:

> "*I have two different lives – social lives on social media where I set privacy – but in reality I am more private. There are more steps in this privacy con-*

> *cept – as I experience in my daily life. Instagram is a laisse-faire media – which stages privacy. For me that doesn't represent 100% privacy*". (Person 7)

> "*In my Instragram profile I am not private while in my Facebook profile I am very private. It depends on where I am. You adapt to the fora*". (Person 8)

> "*I only place things on social media that is okay for me to be shared. I have chosen before I place it there*". (Person 6)

These answers, in which privacy levels are seen relative to the platform used, suggest a perception of privacy as an instrumental – and relative – value. This supports the idea of the bargain of data. Users might however not be aware that data brokers might collect data across platforms, thus short-circuiting the assumed privacy level.

Some of the respondents have experienced direct attacks on their privacy – like stolen passwords, hacks of accounts and once a boyfriend's picture from LinkedIn suddenly was used in a dating profile (referring to question 7). All incidents were handled by contacting the service provider or closing down accounts.

Introducing the concept of data brokers, the respondents were then asked about their opinion on that companies have an interest in their private data and earn money on it (question 10). Most of the respondents were aware of this but have accepted this as part of the game being online and using the services. The answers reveal both instrumental and intrinsic perceptions of the value of privacy:

> "*I have accepted it. For me it is just statistics. I do not feel touched by it. I know it and that is how it is – otherwise I cannot use the Internet*". (Person 7)

Others expressed irritation and frustration about this:

> "*A bit annoying. Even the personalised adds are actually quite annoying – I do not get better services*" (Person 1)

> "*They can do this if they want to pay for it. If it has a value for them, they must pay in one way or another – not necessarily money*". (Person 2)

> "*Maybe they are right in some way – but I do not like this. It is opposite to privacy*". (Person 3)

> "*I noticed that for example they modify the ads to get your interests. It feels like they enter my private space. They get too close to me*". (Person 5)

The statement from person 2 is clearly instrumental in its privacy perception, as well as person 7 who also express a risk-based perception (cf. [30]). The statement from person 1 could also be described as instrumental in its privacy perception, however showing dissatisfaction with the asymmetric power-balance between users and data

brokers. On the other hand, the statements from persons 3 and 5 point at privacy as an intrinsic value. Along with Moor [20], they feel uncomfortably however without being able to point at any other harm than annoying adds. The statement by person 5 "*They get too close to me*" points however at something essential: The individual autonomy like in Moor's reflections. Legally, privacy may not be harmed, but the feeling of loosing autonomy is clear, cf. Brey [5]. For this kind of intrinsic value of privacy a psychological framework might be useful, cf. [26]. The scope of this article allows us however not to elaborate on this, but this might be an important key to the understanding of the perception of privacy as an intrinsic and very precious value.

The respondents were asked about their interest in selling their own data and generally (question 11), and they were not generally not interested:

> "*No, no that is privacy. I do not want that*". (Person 2)

Clearly seeing the privacy as an intrinsic value.

Others thought about the situation where they should sell data to some kind of organisation they should trust with private data and were sceptical about this:

> "*These companies should then buy from me – and lie to me, to persuade me to sell to them. For that is what they do. I do not think I would boarder with that. It would be too much to think about*". (Person 9)

> " *It is a bit funny but I would then be more critical about it where it would go*". (Person 10)

These respondents perceive the privacy risk-based and as an instrumental good but their real problem is apparently the lack of trust to the data brokers. Following up with the question on whether they would allow another company access on their private data for a fee every month (question 12), the respondents generally did not like the idea both out of not seeing the need for this service but also because they would not trust such a company:

> "*It is not something I have a need for – it is a bit frightening*" (Person 2)

> "*I would not trust them*". (Person 6)

> "*This is homburg. There are no companies that can control that at all. It would be very dependent on the company*". (Person 8)

The lack of trust in this trade can be explained with Moor [20] through the concept of greased data. The asset – the personal data – is simply difficult to guard in economic sense, since the seller – the user – have no or few means to verify that the sold object – the personal data – is not being re-sold against contract terms. It cannot be traced, and the value of the assets slips away as grease. Furthermore, the scepticism echoes discussion of trust in e-commerce, cf. [3], [9] and [25]. The conditions for trust, as well as the fair negation of trade conditions between consumers and data brokers are however a big topic that deserves further research beyond this paper.

The respondents were asked whether they would pay a company to take care of their privacy – and what they would be willing to pay for that (question 13):

> "*No I do not think you should pay for your privacy*". (Person 1)
>
> " *As my economy look now, it would be a now - if I got a better economy, then perhaps*". (Person 4)
>
> "*I would need a scare before – if I experienced misuse but otherwise not*". (Person 12)

Here the respondents see differently on the privacy – the person 1, see privacy as an intrinsic value while the persons 4 and 12 can see privacy as instrumental. The persons 4 and 12 do in that way open for the idea of the bargain under the right circumstances.

The final question (question 14) related to "*if you can see yourself in a situation where you would negotiate with a company or institution about the costs of your private data?*" Since this was an idea that the respondents not have heard about before, it was discussed amongst the respondents as a future service:

> "*That sounds reasonable – understood in such a way that you still can have the freedom to say no*". (Person 2)
>
> " *I can see that perhaps happen in 20 years. I think people deserve that… People create the value into the platforms. I think that they deserve a part of the money*". (Person 4)
>
> "*No that I would not be able to imagine. It would be strange*". (Person 5)
>
> "*Practically, that would be completely confusing*". (Person 8)
>
> "*That would be like selling a part of yourself*". (Person 9)
>
> " *I would completely sell out if I could save some money. But it is a disguising thought to sell yourself in that way*". (Person 11)

The respondents have generally a hard time understanding how the bargain would work and how they would be able to manage that situation. It would clearly be much more complex than the situation, they are used to. More respondents mention that they discard the idea about selling private data themselves since they talk about selling themselves in that process. Most of the respondents reject the idea of the bargain of private data. A few (persons 2 and 4 – from question 12 above) can see it happening – not because of a need but because of the trends and technology changes. In particular person 4 doesn't really accept or reject the idea but sends it to the future to "buy himself" more time in relation to understanding the challenge of the bargain.

5 Discussion

The analysis of the interviews shows that privacy is a concept that is understood in different ways. The instrumental versus intrinsic value of privacy is here a good analytical tool to understand the large differences in the interviewee's positions.

The respondents as such are reluctant to accept the data bargain or discard the very idea. Those with an instrumental perception of privacy see the concept as too complex and impossible to administer. Those with an intrinsic perception of privacy discard the idea completely. This is in some ways in big contrast to the fact that data brokers' existence today and that the services are on their way. The respondents haven't thought about this in explicit ways and therefore have a difficult time in understanding the possibilities.

Moor's [20], way of seeing privacy as core value for societal co-existence is not very present in the respondents' answers. They primarily perceive privacy from an individual perspective. Some of the respondents talk about having differing levels of privacy – in real life and on different social media platforms, echoing Goffman [11]. This is another perspective of the adoption to trends and society where the online privacy adapts to the platforms with different levels of privacy. If the trends in society will go towards a more proactive self-administering of private data, bargain situation is still a possibility and cannot be rejected as a future new service. Of course it can be discussed whether these services are premature in their approach to individual control of privacy.

The situation today where online users either need to accept service providers' use of private data or not use the service at all, it is a situation that the respondents clearly have accepted. Several of the respondents in the interview mention that they accept this to use the services. At the same time, this provides asymmetry in the way they perceive privacy and changes their perception of this.

6 Conclusion

User privacy is a difficult concept to manage. It is adjusted continuously according to trends in order to be part of the online society. However, most users are aware of privacy to some extent but have difficulties in understanding the complexity of managing this online. The concept of bargain is too complex for most users to accept.

There is a need to educate users about the challenges in privacy when they use online services. This paper shows that users are aware of privacy but only to a certain level and that they do not necessarily understand the full picture of privacy. They see it as a necessary evil or condition to be part of the social media – but are on the same side also annoyed and frustrated about the data brokers and how they seem to violate the users' privacy.

Visualization tools, as described in section 3, is of course one way forward. With these tools, users can get a visual overview of elements of privacy relating to specifically the data brokers. However, these tools can be difficult for normal users to understand and act upon, so there is a need for taking these tools further to simplify to support the users further. Also these tools only look at part of the privacy picture and there should be services that secure the users by default. The element of the bargain as discussed here, should also be visualised and in that way make it more understandable for the users.

This paper also discusses the idea of payment-based protection of privacy. While the intrinsic-oriented users reject this idea completely, the instrumental-oriented users see the preservation of user privacy as a function of their economy. If they do not have so much money, the online services that require some sort of payment are immediately discarded. This means that there is a risk that there will be a societal gap – a new digital divide - where some users can afford controlling their private data using paid services, while others just go with the flow and adapts to violations of their privacy. With Moor's idea of privacy as a core value for society, the payment-based privacy is not very appealing; reversely it is well in line with Thompson's risk-based approach. Again, we should distinguish between personal data that can be related to a specific person, and personal (consumer-) data that is informing marketing and trend research. The respondents' reactions to privacy cuts however across this distinction. This calls for future services, where privacy is set by default and then can be opened according to the individual's preferences.

The trust in online services is central in this. This term has not been discussed in this paper, but is closely related to the perspective of privacy and the example of the data bargain. There is a paradox in the way that users accept the privacy settings of the services that at the same time want to explore their private data. The element of trust in this relation should be researched more. Also the trust issue should be compared to the trust that any user balances when engaging in online shopping and is a perspective for future research.

References

1. Anton, A.I., Earp, J. and Young, J.D.: How Internet Users' Privacy Concerns Have Evolved since 2002. The IEEE Computer and Reliability Societies, January/February (2010).

2. AVG PrivacyFix: http://www.avg.com/ww-en/privacyfix (2014).

3. Beatty, P., Reay, I., Dick, S., Miller, J.: Consumer trust in e-commerce web sites. ACM Comput. Surv. 43, 1–46 (2011).

4. Branagh, E.: Selling your digital soul – what is your data worth? https://www.cable.co.uk/feature-complex-issues-online……. (2014).

5. Brey, P.: Freedom and Privacy in Ambient Intelligence. Ethics Inf. Technol. 7, 157–166 (2005).

6. Electronic Frontier Foundation/Privacy Badger: http//www.eff.org /privacybadger

7. Federal Trade Commission: Data Brokers. A Call for Transparency and Accountability. (2014).

8. Gates, C. and Matthews, P.: Data is the New Currency. NSPW'14, September 15-18, 2014, Victoria, BC, Canada. ACM 978-1-4503-3062-6/14/09 (2014).

9. Gefen, D.: E-commerce: the role of familiarity and trust, (2000).

10. Glancy, D.J.: Privacy and the Other Miss M. North. Ill. Univ. Law Rev. 401, (1990).

11. Goffman, E.: The presentation of self in everyday life. Doubleday Anchor Books, Garden City (1959).

12. Gosk, S. Stores may be tracking you through your cellphone. http://www.today.com/money/stores-may-be-tracking-you……, (2013).

13. Guest, C., Bunce, A. and Johnson, L.: How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. Field Methods, Vol. 18, No. 1, pp. 59-82, February (2006).

14. Hogan, B.: The Presentation of Self in the Age of Social Media: Distinguishing Performances and Exhibitions Online. Bull. Sci. Technol. Soc. 30, 377–386 (2010).

15. Johnson, D.G.: Computer ethics. Prentice-Hall, Englewood Cliffs, NJ (1994)

16. Khajuria, S. and Sørensen, L.: Where Does My Private Data Go – Visualizations of Users' Privacy. Presented at the HICSS Conference (2015).

17. Koerber, A. and McMichael, L.: Qualitative Sampling Methods: A Primer for Technical Communications. Journal of Business and Technical Communication. Vol. 22, No. 4, pp. 545-473 (2008).

18. Kvale, S. and Brinkman, S.: InterViews: An Introduction to Qualitative Research Interviewing. Thousand Oaks, London, New Delhi: Sage Publications (2009).

19. Lee, T.B.: Here is Everything We Know About PRISM To Date. The Washington Post. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/ (2013).

20. Moor, J.H.: Towards a theory of privacy in the information age. ACM SIGCAS Comput. Soc. 27, 27–32 (1997).

21. Mozilla Lightbeam: http://mozilla.org/en-US/lightbeam (2014).

22. MyPermissions: http://mypermissions.org/ (2014).

23. PC: http://www.pcworld.com/article/2147306/f-secure-freedome-review-vpn-and-security-for-mobile-devices.html (2014).

24. Petty, R.D., D'Rozario, D.: The Use of Dead Celebrities in Advertising and Marketing: Balancing Interests in the Right of Publicity. J. Advert. 38, 37–49 (2009).

25. Ren, Z., Hassan, T.M.: Trust in e-Commerce. e-Business in Construction. pp. 195–210 (2009).

26. Shoemaker, D.W.: Self-exposure and exposure of the self: informational privacy and the presentation of identity. Ethics Inf. Technol. 12, 3–15 (2009).

27. Simonite, T.: Sell Your Personal Data for $8 a Month. MIT Technology Review. http://www.technologyreview.com/news/524621/sell-your-personal….. (2014)

28. Sørensen, L., Nicolajsen, H.W., Bjørner, T.: When Short and Many is Better than Long and Few – Doing Convenience Interviews in Public Places. In: Bjørner, T. (ed): Qualitative Methods for Consumer Research: The Value of the Qualitative Approach in Theory and Practice. Copenhagen. Hans Reitzel, p. 161-166 (2015).

29. Terms of Service Didn't Read: https://tosdr.org/ (2014).

30. Thompson, P.B.: Privacy, secrecy and security. Ethics Inf. Technol. 3, 13–19 (2001).

31. Tufekci, Z.: Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bull. Sci. Technol. Soc. 28, 20–36 (2007).

32. Vedder, A.: KDD: The Challenge to Individualism. Ethics Inf. Technol. 1, 275–281 (1999).

33. Warren, S.D., Brandeis, L.D.: The right to privacy. Harvard Law Rev. 4, 193–220 (1890).

Annex : Interview guide: What do you think about online privacy?

Currently there have been many stories about violation of privacy on social media. The purpose of this interview is to hear what you think is privacy and whether you think there can be money involved in exchange of private data. The interview is a part of research made at Aalborg University. The responses will be used anonymously and only for the purpose of this research. The interview will take around 10 minutes. We appreciate you taking the time.

1. What is your gender (male/female)

2. What is your age (20-25, 26-30, ….)

3. On average how many hours do you use the Internet? (app hours per day)

4. What do you use the Internet for? (as many as possible- social media, browsing, shopping, …….) – which social media do you have profiles on?

5. Do you take any action to protect your privacy while you use the Internet? Which? – Why not?

6. Do you protect your social media profiles in any way? Public open?

7. What kind of information is available to others? Pictures? Birthday dates? Address? Phone number? Real name? e-mail address? Interests? Others?

8. How do you think about the handling of privacy on social media – easy, difficult other?

9. Do you think it is okay to share these data with others?

   9.a What does the word privacy mean to you? Use your own words

   9.b Have you ever experienced any problems with your privacy online?

10. As you may know there are many companies who have an interest in your private data and will earn money on them. They sell them to others who can use the data to target you with for example adds and other things. What do you think about that?

11. If you could would you be interested in selling your data? To whom? What should be the price for an e-mail address? Your address? Personal number? GPS coordinates?

12. A number of services exist, for example Lightbeam, which will pay you for providing them access to your private data (so they can use them as they want – to sell to third parties). The payment is around 10 $ per month). What do you think about that?

13. If we turn the above around we could also ask you whether you would be interested in paying for keeping your private data for yourself (meaning that no one would sell your data further). What should that cost for you?

14. Could you see yourself in a situation where you would negotiate with a company or institution about the costs of your private data? If for example you are buying something in a shop and they want information such as telephone number and you cannot see they should be using that.