Polycentric governance of organizational data ventures

An organizing logic for data governance in the digital era

Benfeldt, Olivia

Publication date:
2020

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

POLYCENTRIC GOVERNANCE OF ORGANIZATIONAL DATA VENTURES

AN ORGANIZING LOGIC
FOR DATA GOVERNANCE IN THE DIGITAL ERA

BY
OLIVIA BENFELDT

DISSERTATION SUBMITTED 2020

AALBORG UNIVERSITY
DENMARK

POLYCENTRIC GOVERNANCE OF ORGANIZATIONAL DATA VENTURES

AN ORGANIZING LOGIC FOR DATA GOVERNANCE IN THE DIGITAL ERA

Olivia Benfeldt

AALBORG UNIVERSITY
DENMARK

Dissertation submitted 2020

.

Dissertation submitted:	September 2020
PhD supervisor:	Associate Prof. John Stouby Persson, Aalborg University, Denmark
PhD co-supervisors:	Associate Prof. Sabine Madsen, Aalborg University, Denmark
	Full Prof. Lars Mathiassen, Georgia State University, USA
PhD committee:	Professor Jeppe Agger Nielsen (chair) Aalborg University
	Professor Ioanna Constantiou Copenhagen Business School
	Professor Leif Skiftenes Flak University of Agder
PhD Series:	Faculty of Social Sciences, Aalborg University

ISSN (online): 2246-1256
ISBN (online): 978-87-7210-700-4

Published by:
Aalborg University Press
Kroghstræde 3
DK – 9220 Aalborg Ø
Phone: +45 99407140
aauf@forlag.aau.dk
forlag.aau.dk

Printed in Denmark by Rosendahls, 2020

Standard pages: 230 pages (2,400 characters incl. spaces).

til mor, far, bidder og sille
mine fire verdenshjørner

ABOUT THE AUTHOR

Olivia Benfeldt has conducted research within the information systems discipline since 2016. She is driven by the desire to understand data as a fast-growing, constantly changing set of digital practices, that is fundamentally changing the way societies and organizations work. Olivia is driven by questions such as: How can we use data-centric technologies to do better, think differently and break new ground? How can we promote accountability, robustness, privacy, freedom, anonymity and unpredictability in a hyper-datafied world?

She approaches these questions with deep interdisciplinarity; shaped by a background in information systems, political science and language as well as her joint affiliation with both the Department of Politics & Society (since 2016) and Department of Computer Science (since 2018) at Aalborg University. Inspired by engaged scholarship, she conducts her research in close collaboration with IT professionals, continuously seeking to bridge theory with practice. Although a scholar at heart, she believes truly interesting problems - and solutions - come about, when researchers and practitioners work closely together. Olivia holds an MSc in Information Technology (2018) from Aalborg University.

ABSTRACT

Technological advancements have enabled the collection and storage of more data than ever before, but datafication expands what can be known about social life. New concerns for data rights, ethics and privacy put immense pressure on organizations to know exactly what data they process, how and for which purposes. Data governance is emerging as a dedicated approach, but insights remain fragmented and studies lack original theorizing. To provide an integrative understanding and a basis for managing the implicated competing concerns, this dissertation seeks to theorize an organizing logic for data governance, which can evolve and enable organizations to confront, govern and resolve growing tensions and devise appropriate rules for data use in the digital era.

As a first step, this dissertation proposes *data ventures* as an intellectual vehicle for explaining the self-rising, organizational arenas, in which individuals negotiate competing concerns for data use as they emerge in practice. Drawing on foundational themes from research on polycentric governance in self-organizing resource systems, this dissertation then undertakes an empirical analysis of a two-year (2017-2019) qualitative, case study focusing on how data governance arrangements evolve before, during and after formal instatement of GDPR (May 2018) within the Danish municipality Fairview. Relying on longitudinal insights, the empirical analysis offers a processual account of how tensions emerge, how dedicated data ventures unfold and are brought into being to negotiate competing concerns and how appropriate data governance arrangements are devised in response.

Leveraging the empirical analysis with extant literature, this dissertation theorizes polycentric governance of data ventures to explicate how a polycentric organizing logic evolves and enables Fairview to devise appropriate data governance arrangements. Data ventures are brought into being as self-rising, situated, arenas in which strategic and operational decisions, social and digital practices are enmeshed to devise appropriate data governance arrangements, while five organizing patterns of polycentric governance are progressively enacted within data ventures and across the organization to facilitate deliberate and emergent organizing of data governance activities.

By introducing polycentric governance of data ventures as a novel theorization, this dissertation extends research on traditional, hierarchical approaches. Data ventures bring attention to how data-related activities emerge, interweave and unfold in situated work practices, while polycentric governance contributes with a processual perspective on how data governance arrangements may be adapted and evolved progressively; over time, in response to rapid external change or emerging internal tensions; and outside organizational boundaries to orchestrate inter-organizational governance arrangements. Together, these insights contribute to broader IS literature by reestablishing data governance as a fast-growing, constantly changing set of digital practices involved in the organizing of data.

DANSK RESUME

Teknologisk udvikling har muliggjort indsamling og lagring af mere data end nogensinde før, samtidig med grænserne flyttes for hvad der kan 'dataficeres'. Øget opmærksomhed på datarettigheder, -etik og privatliv, lægger pres på organisationer, der skal dokumentere præcis hvilke data, de behandler, hvordan og hvorfor. Data governance fremstår som en lovende tilgang til det at navigere potentielt, modsatrettede interesser, men forskningsområdet er fragmenteret og de fleste undersøgelser mangler dybdegående teoretisering. For at udvikle en samlet forståelse, søger denne afhandling at udvikle tidssvarende organisering af data governance, der gør det muligt at konfrontere, styre og manøvrere opstående, modstridende interesser samt at udforme passende forvaltningspraksis af data i et digitaliseret samfund.

I første omgang udvikler afhandlingen begrebsapparatet *data ventures,* for at forklare den selvopstående organisering, hvor i forskellige aktører forsøger at forene modsatrettede interesser og spændinger i arbejdet med data, som disse opstår i praksis. Med udgangspunkt i teori om polycentrisk ledelse af selvorganiserende systemer tilvejebringer afhandlingen en empirisk analyse af et toårigt (2017-2019) kvalitativt, casestudie med fokus på hvordan data governance udvikles før, under og efter indførelse af persondataforordningen (maj 2018) i den danske kommune "Fairview". Gennem en længdesnitsundersøgelse giver den empiriske analyse indblik i hvordan spændinger opstår, hvordan tilsvarende data ventures udfoldes og bringes i anvendelse for at kunne manøvrere de mange, modsatrettede interesser, samt hvordan data governance udformes herefter.

Denne afhandling bidrager således med en dybdegående teoretisering af polycentrisk styrede data ventures for at forklare hvordan organisering af data udvikles og gør det muligt for centrale organisatoriske aktører at udforme passende data governance. Data ventures bliver til som spontant opstående, situeret organisering, hvor i strategiske og operationelle beslutninger sammenvæves med social og digital praksis for at kunne udarbejde passende data governance. Herudover, frembringes og udvikles fem polycentriske handlingsmønstre gradvist på tværs af organisationen, for at kunne imødekomme opstået og planlagt organisering af data governance aktiviteter.

Forskningsmæssigt bidrager afhandlingen til data governance litteratur, hvor den, med sin teoretiske ramme for polycentrisk ledelse af data ventures, udvider eksisterende modeller for hierarkisk organisering. Data ventures giver indblik i, hvordan organisering af data opstår, sammenflettes og udfoldes i arbejdspraksis, mens polycentrisk ledelse bidrager med et procesperspektiv på, hvordan data governance kan tilpasses og udvikles gradvist over tid, for at imødekomme markante, eksterne forandringer og interne spændinger. Tilsammen bidrager disse indsigter til en bredere litteratur om informationssystemer ved at etablere data governance som hurtigt voksende, konstant foranderlige sæt af digitale praksis, involveret i organisering af data.

ACKNOWLEDGEMENTS

As I put together these acknowledgements, I have to recognize the Aalborg University institution. Eight years ago, I set foot on campus as a fresh-faced, first generation university student. I don't remember doing a lot of homework or attending many classes, but I'll never forget camping out in the library three months every single semester to do semester group projects. My fellow collaborators and dedicated supervisors through the years, you paved the way. I remember each of those projects to this day and they remind me why I fell in love with research.

Now on my way to pursue an actual career in academia, I can honestly say: came for the learning, stayed for the people. Any doctoral student will attest that a PhD is not at all fun and games and like many others, I seriously pondered leaving. In hindsight, it's clear that I didn't because I was fortunate enough to become part of the Human Centered Computing group at Department of Computer Science. The social fabric of the HCC group is distinctive and remarkable, made of smart people and cool ideas, but more so than anything; it's made of generous individuals. Cherished HCC colleagues, I've found unmatched solace and inspiration in knowing all of you as friends. Thank you for taking in a stray.

There simply wouldn't be a dissertation, if not for the countless practitioners from various Danish municipalities, who have so generously offered their time and perspective, through the past four years. Your contributions have been invaluable. A special thank you to the Digitalization director and the Information security coordinator in Fairview, who made me feel like a fellow colleague.

As I count my blessings, I'd be remiss not to acknowledge another institution, namely Professor Lars Mathiassen. Whenever we speak, you give me the distinct feeling that for all the hard work and mental perseverance it takes, doing profound, high-impact research is really just about having a good time with your friends, learning about exciting stuff. I vividly remember the fateful day we bounced around in literature and came up with data ventures. Lars, you set high standards for academic scholarship, mentorship and friendship, and I'm very grateful you see something of that in me. Had you not invited me to come work with you in Atlanta, I also never would've met the one and only Kathrine Stampe. Kathrine, I know you despise the idea of being featured in an acknowledgements section, but not mentioning you would simply be not properly citing my sources. You're a whole bunch of inspiring things; fun, big-hearted, systematic, disciplined, able to run 15 km at a 4:00 pace and an incredible mother to your daughter. I don't quite have words for what it means to have met you, but I'm legit excited our perfectionist streaks reverberate at a higher frequency.

Undertaking a PhD means you need a dissertation supervisor, but as the old saying goes: all good things come in threes. Why settle for one, if you can be advised by three brilliant minds. Pernille, even though you left before it all began, you invented me as a PhD student, and for that I'll always be grateful. Your ability to integrate theory with practice is an ongoing source of inspiration for me. Sabine, you have, perhaps unknowingly and more than anyone else, taught me how to maneuver the inescapable pretentiousness of academia. Both in real life and in research. I will never again write another paper without sprinkling a few 'this means that's, whenever it all becomes too high-strung. John, I'm not oblivious to all the times I did the exact opposite of what you told me, but know that you have at least succeeded in teaching me three things: how to stay humble to the task, the subtle art of 'good enough' and, above all, that feelings of inadequacy can be a force for good. I'm grateful you stuck with me throughout all four years and I'm proud to be the first generation in your academic genealogy.

Perhaps no one deserves my gratitude more so than my family. My mom and dad, who have always let me be who I needed to be; your unconditional love and tolerance is the foundation upon which all my future accomplishments are build. My beautiful sisters, Victoria and Cæcilia, who made me an oldest sibling (by trait, not by title); your kindness, your empathy and your resilience reminds me that I'm not the smart one. You're both infinitely wiser than me.

Doing a PhD is many things, but getting it done is probably the hardest. Writing the last words of these acknowledgements means I'm in the homestretch of a weird mix between a marathon and a sprint. Here, I must dedicate a very special thank you to someone who showed superhuman patience with an insufferable, know-it-all. My precious, gentle Rikke; your unwavering confidence that I could pull this off has been invaluable. Thank you is, but a poor word.

Olivia Benfeldt

Aalborg, August 2020

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

CHAPTER 1. INTRODUCTION

1.1. ORGANIZING DATA USE FOR THE DIGITAL ERA

Technological advancements have enabled the collection and storage of more data than ever before with the potential to transform societies and organizations (Constantiou and Kallinikos 2015; Markus 2015; Pereira et al. 2017). The exploitation of data has become fundamental specifically to how organizations operate and compete (Kiron 2017; Kiron et al. 2014; Ransbotham et al. 2016; Ransbotham and Kiron 2017). Yet, to benefit from data-centric opportunities, organizations must be deliberate in the way they organize, analyze, and deploy their data (Porter and Heppelmann 2014, 2015). This task cannot be left to the traditional IT function (Marchand and Peppard 2013). Rather, organizations need an overarching direction for how they orchestrate their data-related activities (DalleMule and Davenport 2017).

Data governance is emerging as a dedicated approach to coordinating and organizing data-related activities on a company-wide scale (Khatri and Brown 2010; Otto 2011a; Ransbotham and Kiron 2017). No consensual definition has been established (Al-Ruithe and Benkhelifa 2017; Brous et al. 2016), but authors agree it involves the design and implementation of rules and responsibilities, which specify how data as organizational assets may be treated (Abraham et al. 2019). Data governance is moving up the corporate agenda for several reasons. Growing data volumes from diverse sources compromise data quality (Otto 2015) and escalate risk exposure (Morabito 2015), while impact of regulatory requirements such as the General Data Protection Regulation (GDPR) (European Commission 2018) put pressure on organizations to know exactly where data is stored, how it is used, who can access it and for which reasons.

Yet, deeper challenges persist. Data governance frameworks remain prescriptive and unilateral in nature (Begg and Caira 2011; Buffenoir and Bourdon 2013), leading their recommendations to disregard the complexities of the meaning of data in practice (Benfeldt et al. 2019). According to a recent survey of Chief Data Officers (CDOs), data governance may well be the solution to aligning data programs with business strategies, but they emphasize building relationships, establishing trust and determining business oriented data needs over 'governance' per se, as this nomenclature has become "somewhat toxic" (Davenport and Bean 2020, p. 7). Practical experiences consistently find mobilizing an organization to follow formal data principles is difficult (Ladley 2012; Vilminko-Heikkinen et al. 2016a), taking stock of data inventory (in order to govern it) remains tedious (Ransbotham et al. 2016) and the importance of investing in such efforts is understood only if a company has already suffered major data breach (DalleMule and Davenport 2017).

Organizations need an overarching direction for orchestrating their data-related activities in the digital era. Data governance is emerging as a viable approach, but significant

challenges abound. It is the purpose of this dissertation to advance knowledge on how organizations can devise appropriate governance arrangements for data in the digital era. The following sections will elaborate on current challenges in practice and enduring issues in research to emphasize the need for pursuing this agenda.

1.2. PRACTICAL CHALLENGES

As data is proclaimed the most valuable resource in the world (Economist 2017), becoming "data-driven" seems to be the new corporate nirvana. Although organizations are keen to pursue data-centric opportunities, evidence from international and Danish contexts indicate that orchestrating the necessary data-related activities on a company-wide scale remains one of the most pressing issues for practitioners in both private and public sectors.

From an international perspective, the Society for Information Management (SIM) has since 1980 been conducting an annual survey of key issues facing IT executives. Based on surveys from 793 organizations between 2008-2018, three of the top ten most important IT management issues related to organizational aspects of data in some way (see Table 1) (Kappelman et al. 2019). While data analytics and data management place #3, this issue did not even figure in the top 10 before 2017, and Security, cybersecurity and privacy jumped from #8 in 2008, to being #1 in 2018 (Kappelman et al. 2019, p. 52). When asked about current and future largest IT investments, IT executives rated data analytics as top of the list, while cybersecurity remained #2, data infrastructure #7 and data integration #11. For organizations, managing data-related activities not only figures as a prominent concern, but also constitute a major financial expense.

#	Issue
1	Security/Cybersecurity/Privacy
2	Alignment of IT with the Business
3	Data Analytics/Data Management
4	Innovation
5	Agility/Flexibility (IT)
6	Compliance and Regulations
7	Digital Transformation
8	Agility/Flexibility (Business)
9	Cost Reduction/Controls (IT)

10	Cost Reduction/Controls (Business)

Table 1. Top 10 most important IT management issues 2008-2018

From a Danish perspective, the consultancy company Ramboll Management Consulting has been conducting a similar report since 1996. For the 2019-2020 investigation, 381 IT and business executives from both private and public enterprises were surveyed on key issues and trends. Five main strategic challenges were established; facilitating 'fast track' digital business development, exploiting blockchain technology, establishing effective cybersecurity, deploying digitalization to facilitate sustainability and aligning expectations in agile development projects (IT in Practice 2019). While the main strategic challenges are not data-related issues per se, eight out of the 11 technologies identified by practitioners as key digital trends were deeply data dependent (IT in Practice 2019, p. 48). These included artificial intelligence (AI), robotic process automation (RPA), big data, Internet of Things (IoT) and blockchain, where a common denominator is that they all require a solid data groundwork:

> "Almost regardless of the digital trend concerned, data constitutes the all-important foundation. The capacity to create value with a given technology depends on the adequacy of the data quality. The enterprises and organizations that successfully translate digital trends into concrete business value are those that actively focus on building a solid data foundation and strong governance" (IT in Practice 2019, p. 47).

Yet, getting a handle on organizational data was deemed a downright "showstopper" for most (IT in Practice 2019, p. 47). The organizational foundation for data treatment and processing was seemingly too inadequate for organizations to engage in strategic exploitation activities with new technologies. In this regard, only 42% of surveyed respondents currently use enterprise data governance and information models, while 81% expect to do so within the next three years (IT in Practice 2019, p. 48). These insights suggest that the need for understanding and developing effective data governance is not only timely and relevant for practitioners in and of itself, but also a prerequisite for pursuing nearly any other technology in the digital era.

Across contexts and sectors, data-centric technologies are pursued for their transformative capacity. Yet, opposition to a reigning techno-optimistic paradigm is also growing, reflecting recent events that have exposed a much darker side of organizational data use.

In 2018, news broke that British firm Cambridge Analytica had illicitly obtained and exploited millions of data points from Facebook users (Rosenberg et al. 2018). Hired to lead social media campaigning for 2016 republican presidential candidate Donald Trump, the company had used the illegally obtained data points to build psychometric profiles on 50 million individual American voters, detailing personality traits such as openness, conscientiousness, extraversion, agreeableness, neuroticism, life satisfaction, political

views and others. Cambridge Analytica used the profiles to identify target audiences, create polarizing digital ads, direct fund-raising appeals, model voter turnout and determine which specific districts would be most susceptible to the republican candidate (Rosenberg et al. 2018). Facebook later came under hard criticism from both British and American lawmakers for failing to discover and deter such data leaks (Rosenberg and Frenkel 2019).

Later referred to as the "Cambridge Analytica scandal", these events were chronicled in the documentary *The Great Hack* (Amer and Noujaim 2019). While exact details of the case remain shrouded in mystery, professor emerita of Harvard Business School, Shoshana Zuboff has deemed the scandal a landmark example of:

> "what living under the conditions of surveillance capitalism means. That every action is being repurposed as raw material for behavioural data. And that these data are being lifted from our lives in ways that are systematically engineered to be invisible. And therefore we can never resist" (Cadwalladr 2019)

Surveillance capitalism, of which Zuboff is the sole progenitor, is an elaborate theoretical framework about the ubiquitous datafication of social life. Here, corporate data accumulation and exploitation specifically is seen as an expression of a new, institutionalizing capitalist logic, which produces hyperscale data assemblages about individuals for the purposes of knowing, commodifying and controlling behavior (Zuboff 2015, 2018). Private corporations unilaterally claim human experience as raw material for amassing and monetizing endless streams of data from users, mostly without their knowledge, understanding, or consent (Sadowski 2019). Optimistic imaginations about these trends become apparent in relentless ambitions to establish smart homes, smart cities, smart governments, and smart healthcare (Kiron et al. 2014), while a countermovement of skeptics warn against growing power asymmetries (Harari 2018), deeper social injustices (Dencik et al. 2016, 2019) and pervasive territorialization (Maguire and Winthereik 2019).

Besides political injunctions against tech giants (Kang and Vogel 2019), mounting techno-skepticism has culminated in the instatement of rigorous data privacy laws that compel organizations to formally govern their data. In effect from May 2018, the General Data Protection Regulation (GDPR) is a European Union directive intended to reshape the way data are handled by any organization operating within the EU, specifically to protect individual data rights (European Commission 2018). Personal data[1] may only be collected and processed if under one of six lawful bases; with consent from the individual, as necessary by a contract with the individual, as part of a legal obligation specified by

[1] Personal data is data relating to a living individual who can be identified from those data alone or from those data in combination with other data, that are *likely* to also exist in the same context

law, to perform interests vital for the individual, as part of a public function or task sanctioned by regulation, and as part of a legitimate interest within the organization (European Union 2016). Data collected under one purview may not be reused in other contexts not covered by the same purview and in the case personal data is compromised, such breaches must be notified to regulatory institutions and affected individuals within 72 hours after. Not only are enterprises fined up to 2-4% of their annual financial turnover (or 10-20 million EUR, whichever is higher) if found in violation, but organizations processing personal data must also be able to at all times demonstrate, they have implemented the necessary technical and organizational governance mechanisms to ensure compliance with the regulation.

Going forward, GDPR and similar frameworks with emphasis on ethics are predicted to fundamentally change the way digital technologies are designed and implemented as information systems in organizations (Addis and Kutar 2018). In the short-term, processing, collecting or exchanging data related to individual behavior, location of personal devices, personal preferences or identities linking to persons will be demanding, but:

> "Trading in personal data and information is not far off. Data valuation will be an independent discipline, where citizens and enterprises will be able to create business models using such means as renting or selling their personal data and information to a third party. Many established IT businesses are already making enterprising attempts to invent new business models in this field. Technologies for processing data and managing the ethical issues these developments are predicted to raise will thus become an independent domain with huge business potential." (IT in Practice 2019, p. 40)

Data philanthropy as the gifting of otherwise proprietary data assets or related knowledge, expertise or tools (Taddeo 2016) is likewise manifesting as a contemporary form of corporate social responsibility. Rising from the ashes of the open data era, data philanthropy shares similar ideals of democratizing data, creating solutions to society's "big problems" and bringing industries together (George et al. 2019). Such public-private data collaboratives will accordingly require sophisticated intraorganizational governance arrangements (Susha and Gil-Garcia 2019).

Organizing data use is challenging in practice and the imperatives are manifold, complex and at times even contradictory. Despite great risks, these data ventures promise even greater rewards. An overarching approach for organizing data in the digital era must necessarily take into accounts the ongoing developments within business, technology, social and political landscapes. Relevant, timely knowledge on how to organize data-related activities is needed to manage the multiple, implicated competing concerns for data use in the digital era.

1.3. THEORETICAL CHALLENGES

Organizational data use is foundational to the Information Systems (IS) research discipline. Acknowledging that data processing systems and organizational tasks are inevitably intertwined lead to the early conception of the information systems concept:

> "A data system cannot produce information, it can only produce data that may represent information to users, i.e. people (or to machines)…The task of any data processing system is to provide information to support decision-making, problem-solving or operational activities; thus such a system can only be really understood as an information system" (Langefors 1977, p. 207)

With the entwining of technology and occupational functions permeating organizations, one common element emerged from these new sociotechnical systems (Baskerville and Myers 2002; Lee 2001); the organizational data resource (Getz 1977). Early IS work immediately observed the inherent difficulties for organizations in managing such a resource. Goodhue et al. (1988) identified five enduring dilemmas of data resource management (summarized in Table 2), which maintains it is not a technology-driven phenomenon, but rather inevitably tied to business objectives and organizational scope. Later, Levitin & Redman (1998) expanded upon the notion of data as a resource to once again establish that:

> "organizational issues contribute to many of the problems (…) Ownership and accountability for data are unresolved issues in most enterprises (…) political battles for control of data and information are among the most brutal we have witnessed (…) Furthermore, the appropriate managerial infrastructure has not yet been determined. The modern hierarchical form may not be suited for the information age." (Levitan and Redman 1998, p. 98)

They add that data like no other resource, by way of its technological subsistence, experiences constant changes in the way it is collected, stored and processed, which is likely to be inherently at odds with stable organizational arrangements (Levitan and Redman 1998).

#	Dilemma	Description
1	Short-term and long-term trade-offs in resource allocation	For investments in data management, managers must decide between activities that will produce immediate benefits and larger infrastructure improvements with delayed cashback
2	The centralizing tendency of data management	Standardization is important for effective data management, but may yield unintended consequences, like monitoring or control by senior management
3	Impact on IS culture	Organizational data management goes against the dominant process oriented IS culture, which has focused on supporting local work practices, not global data flows
4	New responsibilities for user management	Data management is a companywide responsibility, so users and managers in the rest of the organization must develop the necessary data management skills
5	The process of effectively introducing innovations into the organization	Data management efforts often clash with existing cultures, so viewing it as an innovation can help manage the implementation challenges

Table 2. Organizational issues affecting data management

Even so, no converging body of IS literature is explicitly dedicated to advancing knowledge on organizational data use as a sociotechnical phenomenon and related issues remained relatively unexplored within the research field until the big data hype of the early 2010s[2]. Here, the topic saw a massive revival and several calls were made for dedicated IS research on the data phenomenon (Abbasi et al. 2016; Agarwal and Dhar 2014; Goes 2014; Loebbecke and Picot 2015; Sharma et al. 2014). Early papers studying adoption of data analytics seemed again to converge on the realization that business value from data-centric technologies did not materialize from technical implementation itself (Chen et al. 2012; Marchand and Peppard 2013; Ransbotham et al. 2016). Rather, companies were encouraged to define data strategies (DalleMule and Davenport 2017), develop organizational analytics capabilities (Mikalef 2017) establish unified data functions (Porter and Heppelmann 2014, 2015), cultivate data-driven leaders (Fitzgerald 2014; Harris et al. 2010) and hire data scientists (Davenport and Patil 2012; Harris and

[2] Before then, IS research on data seemingly went in other directions. Theories on information as signs carrying meaning (Mingers 1995; Stamper 1991) and technology as sociomaterial artefacts (Orlikowski 1992; Orlikowski and Iacono 2001) distanced the IS field from the data phenomenon, while studies on knowledge management (Galliers and Newell 2001; Markus 2001; Newell et al. 2004), decision support systems (Huber 1981; Silver 1991) and business intelligence (Chen et al. 2012; Foster et al. 2015) assumed data as an organizational resource, without explicitly theorizing about it.

Mehrotra 2014), chief data officers (Lee et al. 2014) and data-savvy board members (O'Reilly and Paper 2012). All this to firmly anchor strategic data use within their organizations.

Meanwhile, data governance emerged as an organization-wide approach to data from various traditions of IT governance, data quality management and information management (Khatri and Brown 2010; Ladley 2012; Otto 2011a). Early conceptions of data governance focused on the implementation of formal rules and responsibilities, which specified decision-making and accountabilities within a series of decision domains regarding an organization's data assets (Khatri and Brown 2010). Much like IT governance (Weill and Ross 2004), data governance emphasized data as an organizational asset with the expressed objective of aligning data activities with business imperatives (Ladley 2012), making it well-suited for providing an organization-wide approach to data use. Scholars have even begun to highlight the potential of data governance for managing issues of privacy, data protection legislation and ethics (Abraham et al. 2019; Vydra and Klievink 2019).

Yet, deeper theoretical challenges persist. A consensual definition of data governance has yet to be established (Alhassan et al. 2019), the topic has received only limited attention in established IS outlets (Nielsen 2017) and the majority of research remains conceptual (Al-Ruithe et al. 2018). Previous work has contributed valuable insights on how to design top-down, organization-wide data governance programs(Brous et al. 2016; Otto 2011d, 2011c; Weber et al. 2009), but others have criticized the dominance of unilateral and normative approaches (Begg and Caira 2011; Buffenoir and Bourdon 2013). The limited view of data governance as a matter of strategic asset management (Mikalef and Krogstie 2020) tends to neglect the informal role of data in day-to-day organizational activities, while virtually no studies engage how data governance unfolds in practice (Alhassan et al. 2016). Empirical studies find that mobilizing organizations to adhere to standardized data principles remains difficult (Nielsen et al. 2018), the value of data as an organizational asset is not immediately clear in practice (Vilminko-Heikkinen et al. 2016a) and organizational members tend not to commit beyond their own group-specific functions (Vilminko-Heikkinen and Pekkola 2019). Remaining focused on decision-making rights and formal roles goes squarely against findings from Levitin and Redman (1998), who indicated hierarchical structures may be inadequate for data resource management in the information age.

Recent developments indicate researchers have begun to explore broader aspects of data governance (Janssen et al. 2020; Mikalef, Pappas, et al. 2020). Recent studies have theorized data governance as an inherent collective action problem, which depend on heterogenous practitioners to adopt cooperative strategies, despite diverging professional or ideological perceptions of data (Benfeldt et al. 2020) and investigated 'data curation' as the everyday manifestation of data governance in local practices for improving data quality, filtering irrelevant data and ensuring data protection (Parmiggiani and Grisot 2020).

Scholars agree that data governance is both promising and necessary in the digital era, but current research remains narrowly focused on rational decision-making structures and proves ill-equipped to cope with the turbulent, multifaceted reality of organizational data use. Insights on how organizations can devise appropriate governance arrangements for data in the digital era are needed to address enduring theoretical concerns about organizational data in IS literature and contribute to a growing research area on data governance.

1.4. RESEARCH QUESTION

In practice, data governance has become a key concern and essential for pursuing nearly any digital trend. New directives for data rights and privacy put immense pressure on organizations to know exactly what data they have and for what purpose this data is used. Yet, practical concerns are unmet by theoretical ideas about how to organize data in the digital era. Though scholars agree that data governance is both promising and necessary, insights remain fragmented and studies lack original theorizing, which limits cross-fertilization and prevents consolidation of empirical findings across contexts (Benbasat and Zmud 2003; Grover and Lyytinen 2015). Knowledge on organizational data use is scattered across diverse research streams and increasingly dichotomized by paradigms of techno-optimism and techno-skepticism, with no theorizing about how these are resolved in practice.

To provide an integrative understanding and a basis for managing the implicated competing concerns, this dissertation proposes that tensions between fundamental assumptions in organizational data use may be confronted, governed and resolved in what is conceptualized as *organizational data ventures*. Building on the notion of a venture as "a risky or daring journey or undertaking", data ventures are theorized as an intellectual vehicle for understanding and explaining how multiple strategic, operational, social and digital practices interweave in self-rising, organizational arenas, as individuals try to cope with uncertainty in practice. Data ventures unfold and can be brought into being as tensions emerge, to negotiate competing concerns for data use and allow appropriate data governance arrangements to be formed and adapted in response.

Traditional data governance models rely heavily on compartmentalization and hierarchical designation of authority and control, but such structures remain insufficient, when data governance (also) depends on distributed outcomes in locally situated, autonomous units (Child and Rodrigues 2003), like data ventures. To accommodate both deliberate and emergent data-related activities, this dissertation seeks to advance knowledge on a corresponding organizing logic (Sambamurthy and Zmud 2000) which can evolve and enable organizations to cope with uncertainty and devise appropriate arrangements for governing the constantly changing set of digital practices involved in organizational data use. Specifically, this dissertation extends previous work on governance in robust, self-organizing resource systems (Ostrom 1990, 2005) to explore *polycentricity* as an apt organizing logic for data governance in the digital era.

Extensive theoretical and empirical research on long-term, sustainability of natural resource systems indicate the underlying rationale for designing and evolving robust, adaptive governance exhibits characteristics of an organizing logic of polycentricity (Ostrom 1990, 2005). In robust socio-ecological systems, local communities self-organize to cope with different threats from the environment, such as free-riding, overuse and pollution and evolve intricate rules for appropriation and provision of a collective resource, such as timber, water, fish or pasture. Similarly, an organizing logic for data governance must necessarily enable organizations to confront, govern and resolve growing tensions arising from inherently competing concerns and devise appropriate rules for data use in the digital era. This culminates in the research question:

RQ: How does an organizing logic of polycentricity evolve and enable an organization to devise appropriate data governance arrangements in response to competing concerns for data use in the digital era?

To address the research question, this dissertation adopts an engaged scholarship approach (Van de Ven 2007) which enables researchers to engage in rigorous theory development, while still addressing relevant, real-world problems anchored in practice (Mathiassen 2017). Foundational themes from research on polycentric governance in self-organizing resource systems inform the empirical analysis of a two-year (2017-2019) qualitative, case study (Yin 2009) that focused on the evolution of data governance arrangements within the Danish municipal organization Fairview, before, during and after formal instatement of the European General Data Protection Regulation (GDPR) in May 2018.

Prior studies on data governance adopt "one-off" or cross-sectional perspectives (Abraham et al. 2019, p. 433), while only a handful of studies reflect how isolated data governance concepts, such as strategy (Tallon et al. 2013) ownership (Vilminko-Heikkinen and Pekkola 2019) and effectiveness (Otto 2013) might need to change over time. In contrast, the empirical study in this dissertation relies on longitudinal insights and situated observations. This allowed a processual account (Van de Ven 2007) of how polycentric organizing patterns evolved throughout key episodes over the two years, including how tensions emerged, how dedicated data ventures unfolded and were brought into being to negotiate competing concerns and how appropriate data governance arrangements were devised in response.

By theoretically and empirically conceptualizing an organizing logic of polycentricity for the data governance context, this dissertation engages in blue ocean theorizing (Grover and Lyytinen 2015) to explicate how organizations can engage in deliberate and emergent organizing of data use through polycentric governance of organizational data ventures. This organizing logic explains how data ventures unfold and can be brought to bear as

self-rising, organizational arenas, in which multiple strategic, managerial, operational, social and digital practices are enmeshed by individuals to devise appropriate data governance arrangements in response to competing concerns, and polycentric organizing patterns are progressively enacted within data ventures and across the organization to coordinate both deliberate and emergent data-related activities.

1.5. DISSERTATION OVERVIEW

The primary objective in this dissertation is to advance knowledge on data governance by theorizing a corresponding organizing logic for the digital era. As such, the structure of the dissertation does not reflect the chronological research process but seeks to gradually unfold and explain this logic in a comprehensible manner to the reader. In doing so, the dissertation consists of seven chapters, each different in character and intent.

Chapter 1 Introduction frames the dissertation by sketching key challenges in practice and research related to organizational data use and governance. The chapter anchors the research effort in a real-world problem, briefly summarizes fragmented insights in existing literature, proposes a theoretical framing and culminates in the formulation of the research question.

Chapter 2 Literature Background first takes the reader through insights on organizational data use across existing literature to position data governance and thus the contribution of this dissertation. A review of data governance literature details a budding, research area and coins the novel term 'data ventures' to explain how data governance can be spontaneously formed, adapted and evolved through various activities in practice. The chapter concludes with a reconceptualization of data governance for the digital era and resulting implications for its organizing.

Chapter 3 Theoretical Framing extends research on sustainability of natural resource systems, where self-rising governance arrangements evolve over time to cope with different environmental threats, to theorize polycentric governance as appropriate for organizing data governance. The chapter details how an organizing logic of polycentricity attend to key implications for data governance in the digital era and form the basis of the dissertation's contribution. The chapter concludes with an explanation of key themes and detail how they guide data collection and shape empirical analysis.

Chapter 4 Research Approach details the overall research approach of this dissertation, outlined as a collaborative form of engaged scholarship. A qualitative, single-case study with a process focus constitutes the research design. The case unfolds in the research setting of a Danish municipality, Fairview, where empirical material is generated with practitioners through multiple workshops, interviews, and situated observations. The chapter discusses multiple methodological and philosophical considerations and accounts briefly for the analytical approach.

Chapter 5 Empirical Analysis reports on the case study in Fairview municipality. The analysis details how an organizing logic of polycentricity gradually evolves within the organization, as focal actors engage in deliberate and emergent organizing of data. Empirical evidence show how data ventures unfold and are brought into being as focal actors enact polycentric governance to form, adapt, and evolve various data governance arrangements in response to competing concerns for data use. The chapter is structured according to four episodes identified across the empirical material.

Chapter 6 Discussion leverages key insights from the empirical analysis in combination with insights from extant literature to theorize polycentric governance of data ventures as an organizing logic for data governance in the digital era. The chapter reestablishes the novel concept 'data ventures' and sketches five related organizing patterns of polycentric governance. The chapter ends with a consideration of key implications for practice.

Chapter 7 Conclusion provides a final summary of the work contained in this dissertation in response to the research question. The chapter concludes with a discussion of key contributions and outlines how polycentric governance of data ventures contributes to literature on data governance and advances knowledge on organizational data use.

CHAPTER 2. LITERATURE BACKGROUND

2.1. PERSPECTIVES ON ORGANIZATIONAL DATA USE IN LITERATURE

For scholars addressing problems anchored in real-world settings, positioning new research vis-à-vis existing literature possibly involves combining multiple areas of research as backdrop for making a contribution to literature (Mathiassen 2017, p. 19) While no converging body of IS literature is explicitly dedicated to advancing knowledge on organizational data use as a sociotechnical phenomenon (Newell and Marabelli 2015), related insights are scattered across two parallel research streams (see Table 3).

The first focuses on data-centric technologies for transforming operations, innovation and strategy to create competitive advantage for organizations and solve complex problems in society. New technological developments for data collection, storage and manipulation represent a revolution in the ways organizations make decisions (McAfee and Brynjolfsson 2012), conceive strategic objectives (Constantiou and Kallinikos 2015; Davenport 2014; Woerner and Wixom 2015) and facilitate business innovation (Marshall et al. 2015; Ransbotham and Kiron 2017). Organizational exploitation of data is studied as the use of specific data-centric technologies, such as big data analytics (Gust et al. 2017), virtual and augmented reality (Porter and Heppelmann 2017) and smart, connected products (Porter and Heppelmann 2015) to achieve general, industry specific, operational and strategic goals (DalleMule and Davenport 2017). Google, Facebook, Amazon, Netflix, Uber are often used to exemplify what can be achieved through data-driven ingenuity, while underlying optimistic imaginations about how technologies can favorably transform society become apparent in relentless ambitions to also establish smart homes, smart cities, smart governments, and smart healthcare (Kiron et al. 2014).

Barriers to adoption and value creation in this stream are often attributed to a lack of 'data-driven decision making culture' (Foster et al. 2015), where organizations can resolve by cultivating data-driven leaders (Fitzgerald 2014; Harris et al. 2010), hiring data scientists (Davenport and Patil 2012; Harris and Mehrotra 2014) and attracting data savvy board members (O'Reilly and Paper 2012). Executives are encouraged to pursue data exploitation on behalf of their organization by defining dedicated data strategies that blend 'defense' with emphasis on gaining control and minimizing risk, and 'offense' with focus on improving competitive position and maximizing profitability (DalleMule and Davenport 2017).

Underlying this stream are optimistic assumptions about a new, progressive era, in which the primary objective for all organizations, regardless of industry (Abbasi et al. 2016) is

to unlock the inherent potential of data-centric technologies (Davenport et al. 2012; Kowalczyk and Buxmann 2015).

A second research stream cautions that growing datafication of social life is not inherently desirable, but should be rigorously questioned, regulated or even restricted. In this stream, organizational data use is not understood from the point of view of companies looking to derive business value from data-centric technologies as technical artefacts, but rather directs attention to the multiplicitous ramifications of sociopolitical, cultural, economic and ethical nature following from increasing data exploitation in public, private, local, global and governmental organizations. In sum, what happens when evermore aspects of social life becomes 'knowable' (Dencik et al. 2019).

Research	**Area of concern**	**Core idea**	**References**
Data-driven management, data analytics and digital transformation	Data-driven decision making	Studies argue big data enable more accurate insights that lead to better information and better decision making at operational levels	Barton and Court 2012; Davenport 2014, 2013; Fitzgerald 2014; Foster et al. 2015; George et al. 2014; Glasser 2013; Harris and Mehrotra 2014; Jia et al. 2015; Kallinikos and Constantiou 2015; Nicolini et al. 2015; Osuszek et al. 2016; Sharma et al. 2014
	Data-driven business strategy	Studies demonstrate how data-centric technologies enable new strategic positioning and competitive advantage	Abbasi et al. 2016; Constantiou and Kallinikos 2015; DalleMule and Davenport 2017; Ferguson 2014; Fogarty and Bell 2014; Harris et al. 2010; Kiron et al. 2014; O'Reilly and Paper 2012; Porter and Heppelmann 2017; Ransbotham et al. 2016; Ransbotham and Kiron 2017; Woerner and Wixom 2015
	Data-driven innovation and business transformation	Studies argue use of data centric technologies create foundation for radical innovation in organizations and industries	Davenport et al. 2012; Davenport and Patil 2012; Harris et al. 2010; Kiron 2017; Loebbecke and Picot 2015; Marshall et al. 2015; Porter and Heppelmann 2015
	Adoption of data-centric technologies	Studies report on implementation and adoption of specific data-centric technologies in organizations	Gunther et al. 2017; Mikalef 2017; Riggins and Wamba 2015; Tiefenbacher and Olbrich 2015; Vanauer et al. 2015; Wang et al. 2015

Datafication, data politics, and surveillance society	Surveillance capitalism	Studies criticize an institutional capitalist logic of accumulation and surveillance in an information society	Dencik et al. 2016; Knox and Nafus 2018; Reidenberg 2014; Richards 2012; Zuboff 2015, 2018
	Critical data studies	Studies examine critical approaches to study datafication of society, government, industries and organizations	Amoore 2018; Boyd & Crawford 2012; Kitchin & Lauriault, 2018; Reeves 2016; Taylor 2017; Zigon 2018
	Data rights as human rights and social justice	Studies interrogate how specific and general use of data-centric technologies reinforce social injustices	Berry 2019; Bond et al. 2012; Crawford 2014; Kang and Vogel 2019; Martin 2015; Reeves 2016; Reidenberg 2014; Zigon 2018
	Epistemological implications of datafication	Studies question how datafication expands what can be known about social life and implications for privacy and citizenship	Angiuli et al. 2015; Daries et al. 2014; Hintz et al. 2018a, 2018b, 2018c; Kitchin, 2014; Solove 2007, 2012; Sweeney 2002

Table 3. Research on organizational data use

No area of concern illustrates the dangers and irreversibility of corporate data accumulation and exploitation quite like that of Zuboff's (2018) surveillance capitalism. Surveillance capitalism is identified as an unprecedented type of omnipresent logic that allows private corporations to endlessly amass and monetize unending streams of data from users. They unilaterally claim human experience as raw material for hidden commercial practices of extraction, prediction, and sales, mostly without users' knowledge, understanding, or consent (Sadowski 2019; Zuboff 2018). A budding discipline of critical data studies emerges, where data-centric technologies and their pervasive infrastructures are rejected as transparent, objective informational entities and instead investigated as 'assemblages' with agency that inflect and interact with society and individuals (Iliadis and Russo 2016). Social media platforms specifically are interrogated for their ubiquitous data collection, which enables more invisible surveillance (Reidenberg 2014), minority group discrimination (Taylor 2017) and individual privacy infringement (Solove 2007, 2012).

Public-sector digitalization is appraised for its ability to democratize access to and quality of public services in a resource-poor, data-rich society (Reeves 2016), but also criticized for subscribing to a capitalist rhetoric. 'Digital citizenship' (Hintz and Brown 2017) not only envisions the complex lives of multifaceted citizens as passive consumers of public services, but also prevents any individual the ability to opt out. Digital public services rely on corporate technology vendors to mediate often personal, sensitive, and intimate interactions between citizens and state; political debates unfold through commercialized social media platforms; election campaigns depend on online engagement, while virtually all human activity is digitally tracked and traced (Hintz et al. 2018a). Besides erosion of citizen privacy and anonymity (Daries et al. 2014), citizenship in a datafied society enables and justifies new forms of governmental dataveillance (Van Dijck 2014) and social sorting (Hintz et al. 2018b) and anticipatory governance (Guston 2014).

More recently, the notion of data justice has emerged to capture how preexisting racial and sociocultural biases tend to become embedded in certain data-centric technologies, like facial recognition software or artificially intelligent chatbots (Berry 2019; Crawford et al. 2014). As public administration pursues data-driven efficiency imperatives, lines blur between predictive analytics and preemptive governance, where citizens are managed as risk-scores before they 'do something' (Dencik et al. 2016). As datafication expands what can be known about social life, corresponding expansions of ethical, moral and existential concerns are required (Zigon 2018). While 'check-list' ethics are appropriate for structuring formal litigation on what can and cannot be done with data, they are insufficient in guiding practices for data scientists, software developers and others developing data-centric technology (Knox and Nafus 2018). Organizations must let go of the idea that ethics can be preprogrammed in rules of universal ideas about 'what is the right thing to do' and instead consider relational ethics, where such ideas are continuously renegotiated in relationships of mutual respect and engagement (Zigon 2019).

Underlying this stream are critical assumptions about organizational data use, as it contributes to a problematic datafication of social life in the digital era. Data-centric technologies enable organizations to claim human experience as the raw material for hidden practices of knowing, controlling, modifying and commodifying human behavior (Taylor 2017; Zuboff 2015).

Across these multiple areas of concern, it is clear that organizational data use is a phenomenon of substantial practical relevance and theoretical significance. Yet, the line between constructive and questionable data use also grows increasingly obscure; predictive disease treatment may regress into health insurance discrimination; personalized web and shopping experiences fuel surveillance capitalist practices and; preventative crime measures easily mask unjust social marginalization (Martin 2015). Within the first research stream, multiple areas of concern in literature seem to favor a hopeful outlook on the value and transformative potential of organizational data use, while perspectives across the second research stream remain unconvinced by techno-

utopian ideals and instead adopt a highly critical stance, pointing to inherent political, ethical, moral and existential dilemmas in organizational data use. Current insights are fragmented, which makes it difficult to systematically confront the growing dichotomy between the hopes of the optimists and the qualms of the critics. In between, data governance is emerging as a promising approach for bridging the two (Abraham et al. 2019; Vydra and Klievink 2019) and providing an overarching direction for how organizations manage the competing concerns of data use in the digital era. The following sections will review extant data governance research.

2.2. DATA GOVERNANCE IN LITERATURE

A budding area of research is emerging with attention to data governance in organizational data use (see Table 4 at the end of this section for an overview). In broad terms, governance may be understood as the process of steering an organization through collective action in accordance with common goals (Torfing and Ansell 2016). Despite growing attention from scholars (see Figure 1), knowledge on data governance remains fragmented (Abraham et al. 2019) without a consensual definition of key terms (Alhassan et al. 2019) and historically receiving limited attention in established IS outlets (Nielsen 2017).

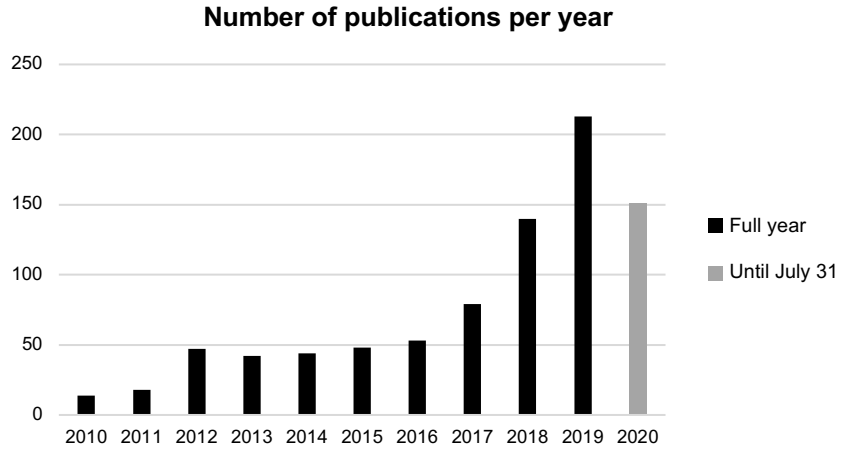

Figure 1. Publications on data governance 2010-2020[3]

Meanwhile, data governance emerged as an organization-wide approach to data from various traditions of IT governance, data quality management and information

[3] Retrieved using dimensions.ai (Hook et al. 2018) on July 31, 2020 specifying "data governance" as search string in title and abstract.

management (Khatri and Brown 2010; Ladley 2012; Otto 2011a). Early conceptions of data governance focused on the implementation of formal rules and responsibilities, which specified decision-making and accountabilities within a series of decision domains regarding an organization's data assets (Khatri and Brown 2010). Much like IT governance (Weill and Ross 2004), data governance emphasized data as an organizational asset with the expressed objective of coordinating data activities with business imperatives (Ladley 2012), arguing treatment of data assets must align with business goals to increase value. Overarching principles, policies and procedures streamline activities for data in an organization, designated across hierarchical functions to ensure enforcement (Brous et al. 2016). In early research, data governance was closely linked to master data management as the processes for changing organizational behavior (Otto 2011d; Wende 2007) to improve data quality on a series of dimensions important for use in context (Liaw et al. 2014; Wang and Strong 1996).

Researchers have started highlighting the potential of data governance for managing complex issues of privacy, data protection legislation and ethics in organizational data use (Abraham et al. 2019; Addis and Kutar 2018; Vydra and Klievink 2019). Although previous work has contributed valuable insights on how to design top-down, organization-wide data governance programs (Brous et al. 2016; Otto 2011d, 2011a; Weber et al. 2009) others have criticized the dominance of unilateral and normative approaches as too narrow (Begg and Caira 2011; Buffenoir and Bourdon 2013; Parmiggiani and Grisot 2020). The limited view of data governance as a matter of strategic asset management (Mikalef and Krogstie 2020) tends to neglect the informal role of data in day-to-day organizational activities, while virtually no studies engage how data governance unfolds in organizational practice (Alhassan et al. 2016).

Despite promising in theory, empirical investigations of data governance report significant challenges. Data does not immediately translate to assets for practitioners (Nielsen et al. 2018) and data governance accountability frameworks remain prescriptive and difficult to implement in complex, organizational realities (Begg and Caira 2011; Vilminko-Heikkinen et al. 2016a; Vilminko-Heikkinen and Pekkola 2019). Even though data governance schemes often adopt rational, unilateral approaches to distributing organization-wide decision making about data, organizational members tend not to commit beyond their own group-specific functions (Vilminko-Heikkinen and Pekkola 2019). Such findings seem to resonate with Levitin and Redman (1998), who indicated hierarchical structures may be inadequate for data resource management in the information age.

Other data governance literature tends to focus on how to increase compliance, transparency and accountability in administration by specifying formal rules for data use (Breaux and Alspaugh 2011). Formal data governance can provide transparency for public sector agencies specifically, which are often subjected to mandated audits of their information practices and required to rigorously document how data are treated in case processing and according to legislative requirements (Dawes 2010; Power and Trope

2006; Thompson et al. 2015). Unsurprisingly, attention to data governance as a research topic increased following official instatement of the European data protection regulation in 2018 (see Figure 1), which puts immense pressure on organizations to know exactly what data they collect, about whom, for what purposes and how these data are processed, both in organizational processes and proprietary IT systems (Addis and Kutar 2018; Farshid et al. 2019; Kurtz and Semmann 2018; Li et al. 2019; Russell et al. 2018). By extension, dedicated frameworks for specific data-centric technologies begin to emerge, with data governance for platform ecosystems (Lee et al. 2018; Nokkala et al. 2019; Tiwana et al. 2010), artificial intelligence (Janssen et al. 2020; Winter and Davidson 2019a), personal health information (Winter and Davidson 2017, 2018, 2019b) and big data analytics (Mikalef, Boura, et al. 2020; Mikalef et al. 2018; Mikalef and Krogstie 2018) amongst others.

Recent research has seen the purview of data governance expand. Beyond traditional governance approaches involving formal principles, structures, decision-making rights and asset management, scholars increasingly pay attention to data governance practices and how these are enacted in various formal and informal organizational arrangements. Such studies assert data are not predefined in governance, but emerge as assets in situated work practices (Monteiro and Parmiggiani 2019) through improvised, everyday data curation activities, such as achieving data quality, filtering irrelevant data and ensuring data protection (Parmiggiani and Grisot 2020). Scholars have likewise examined how data governance is arranged in various organizational forms, either to mobilize collective action within an organization of heterogenous practitioners with diverging professional and ideological perspectives on data (Benfeldt et al. 2020) or to support large-scale, cross-sectorial, interorganizational data use (Winter et al. 2019).

Governing data as an organizational resource has occupied IS researchers for several decades (Getz 1977; Goodhue et al. 1988; Levitan and Redman 1998). Though scholars agree that data governance is both promising and necessary in the digital era, insights remain fragmented and studies lack original theorizing, which limits cross-fertilization and prevents consolidation of empirical findings across contexts (Grover and Lyytinen 2015). Moreover, various perspectives seem to indicate organizational data use is characterized by fundamentally competing concerns, which cannot fully be addressed by established problem-solution patterns in individual areas of concern. The need for original approaches is well reflected within calls for dedicated IS research on data related issues (Abbasi et al. 2016; Goes 2014), and only more urgent as techno-optimism and techno-skepticism grow increasingly dichotomized, with no corresponding understanding and explanation about how to confront and resolve these tensions in organizational practice.

Central assumptions about organizational data use in the digital era are clearly at odds and encounters between them are likely to produce tensions (Mingers 2001) that render data governance highly unpredictable and volatile in practice. In cases of paradigmatic incommensurability, establishing second-order constructs can help bridge differences by

bringing commonalities forth in lower-level concepts (Gioia and Pitre 1990). Consequently, this dissertation propose that the fundamentally competing concerns of organizational data use may be confronted, governed and resolved in what is conceptualized as *organizational data ventures*, detailed in the next section.

Research focus	**Core idea**	**References**
Strategic data asset management	Studies establish conceptual models for how to designate formal roles and decision-making rights for data assets	Alhassan et al. 2016, 2018; Al-Ruithe et al. 2016; Khatri and Brown 2010; Kooper et al. 2011; Lee et al. 2014; Malik 2013; Otto 2011a, 2011b; Pierce et al. 2008; Smallwood 2012; Tallon 2013; Vilminko-Heikkinen and Pekkola 2019
Data quality management	Studies specify how improvement of data quality can increase value of data assets	Brous et al. 2016; Otto 2011, 2013; Panian 2009; Vilminko-Heikkinen and Pekkola 2019; Wang 1998; Wang and Strong 1996; Weber et al. 2009; Wende 2007
Compliance, transparency and accountability	Studies examine how formal governance increase transparency and accountability in data use	Addis & Kutar 2018; Breaux and Alspaugh 2011; Buffenoir and Bourdon 2013; Dawes 2010; Power and Trope 2006; Thompson et al. 2015;
Implementation of data governance in practice	Studies detail practical experiences with implementation of data governance programs in organizations	Alhassan et al. 2019; Alofaysan et al. 2014; Begg and Caira 2011, 2012; Benfeldt et al. 2020; Cheong and Chang 2007; Choi and Kröschel 2015; Haneem et al 2019; Nielsen et al. 2019; Panian 2010; Vilminko-Heikkinen et al. 2016
Formal data governance for specific technologies	Studies develop specific governance frameworks for data in digital platforms, AI, shared data repositories etc.	Mikalef et al 2018; Winter & Davidson 2019b; Janssen et al 2020; Lee et al 2018
Organizational data governance arrangements	Studies explore how data governance is enacted in various organizational forms and work arrangements	Getz 1977; Vassilakopoulou et al., 2019; Winter et al., 2019; Winter & Davidson, 2019a, 2017; Parmiggiani & Grisot, 2020

Table 4. Data governance in literature

2.3. DATA VENTURES AS THE NEW NORMAL

This dissertation builds on the notion of a venture as "a daring or risky journey or undertaking" to theorize *data ventures* as an intellectual vehicle for understanding and explaining the temporary self-rising, organizational arenas, in which multiple managerial, operational, social and digital practices interweave as data governance is formed, adapted and evolved in response to competing concerns for data use from within and outside the environment. In this vein, organizational data use may be understood as both the ongoing activities in and stable outcomes of several uncertain, spontaneous undertakings – data ventures – that evolve to address and overcome unpredictable conflicts; to conquer unexplored land at the expectation of great reward.

With reminiscence of overseas exploration in the Age of Discovery, 'doing' data governance is not the goal itself, but rather the means for achieving all sorts of known and unknown organizational value. In the sense that explorative voyages required extensive preparation and planning to have any chance at success, formal data governance approaches are both necessary and useful, but their narrow attention to stability and rationality means they are ill-equipped to capture the full range of both planned and spontaneous activities involved in organizational data use. Much like thunderstorms, scurvy and mutiny, unforeseen problems that arise from competing concerns for data use in practice cannot be readily resolved in advance through standardized solutions; they require responsive, skillful maneuvering, improvisation and negotiation.

Risky and daring in this sense should not be understood as actual danger or peril, but as characterized by great uncertainty and unpredictability; data ventures unfold and can be brought into being to absorb potential volatility as new arrangements for data use transgress and enmesh with established practices, rules, responsibilities and norms to potentially cause tensions. Data ventures only materialize as self-rising, action arenas, when tensions become salient as competing concerns, but remain open-ended and flexible to co-evolve as practitioners try to negotiate working resolutions to problems.

Another example can be considered as master data management is implemented in an organization. General principles and standardizing data practices are implemented across an organization to improve data quality and facilitate data sharing (Vilminko-Heikkinen and Pekkola 2013). Since day-to-day data curation practices are often co-constituted by work practices (Parmiggiani and Grisot 2020; Vilminko-Heikkinen and Pekkola 2012), local teams and departments inevitably end up with working translations of general principles. This essentially involves a paradoxical, organizational change process (Vilminko-Heikkinen et al. 2016a), where local conditions must be carefully renegotiated without compromising the goals of standardization. Implementations of this nature involve deep changes to roles, responsibilities and ownership, leading to multiple contradictions and conflicts across levels (Vilminko-Heikkinen and Pekkola 2019). Such conflicts can advantageously be approached through orchestration of multiple data

ventures. Here, functioning compromises between global master data management principles and local data-work practices can be negotiated specifically in response to the local challenges that arise, without amending or jeopardizing the overarching standard.

Essentially, data ventures are temporary arenas, but results and outcomes negotiated within them persist or develop into other forms and arrangements, such as new data governance principles, original technical solutions, or even new organizational units (Foster et al. 2015). For example, data analytics refers to a specific set of data-centric technologies used for advanced analysis and understanding of business performance (Chen et al. 2012). To realize value, organizations need to establish dedicated data analytics capabilities which involves leveraging processes, practices, people, skills, technology and culture (Bygstad et al. 2018; Mikalef 2017). Analytics rely amongst others on creative value discovery, open platform architecture and radical data sharing, which are inherently at odds with established organizational concerns for hierarchy, formal decision-making, specialized units, and limited inter-departmental collaboration (Chen et al. 2017). Data analytics as an organizational capability means individuals can access, utilize and transform data into insight through appropriate structures, procedures and roles with regard for security, privacy and ethics, but such projects have known to fail without effective data governance (Mikalef, Pappas, et al. 2020; Tallon et al. 2013). Launching large-scale restructuring projects, where data governance arrangements, business processes and technological skills are planned in advance is both costly, risky and unlikely to succeed (Gust et al. 2017); instead, small-scale technical solutions, tentative process designs, and new cross-functional collaboration forms can be inexpensively tried and tested through experimentation and learning-by-doing in multiple data ventures.

Some formulaic organizational forms dedicated to arranging data use have begun to emerge, including business intelligence and analytics (BI&A) projects (Chen et al. 2012), BI competence centers (Foster et al. 2015) and unified data functions (Porter and Heppelmann 2015). When stable arrangements of this kind cannot be established, data ventures can also emerge to facilitate informal collaboration and skill development. For instance, to package and sell organizational data to others, companies need to refine appropriate processes, skills and culture to generate maximum return (Wixom and Ross 2017). They must also momentarily develop a trust-based relationship with external partners to ascertain legal boundaries, develop non-disclosure agreements and agree on appropriate pricing for their data assets (Najjar and Kettinger 2013). Such exchanges are difficult to formalize in projects or departments, due to their exploratory, open-ended nature. Instead, data ventures can provide enough momentary flexibility to facilitate negotiation and restructuring of resources and develop a data monetization business model which benefits both parties. Similar concerns are involved in data philanthropy, a new form of corporate social responsibility, where corporations donate otherwise proprietary data to other companies, which often involves licensing complementary assets, such as data science expertise, data warehouse access and big data technology, to clean, analyze and use the data effectively (George et al. 2019). Establishing proper data

governance to support data philanthropy will necessarily require situated negotiation and highly contextual arrangements in each instance, since data processing capabilities are likely to vary among the recipients. Data ventures can emerge temporarily to provide the necessary organizing.

As ethics, justice and moral dilemmas come to characterize more data use in the digital era (Dencik et al. 2019; Zigon 2019), data ventures can also materialize to attend to unprecedented or sensitive problem domains, which require contextual consideration and mutual respect. For instance, large-scale health data mining is largely perceived to serve the public with its potential to improve healthcare services, population health, and evidence-based medicine (Alofaysan et al. 2014; Wang et al. 2015). Yet, aggregating personal health data across multiple sources can also embody real risks of countering public good (Winter and Davidson 2018). Health data can be monetized and sold to pharmaceutical companies, who then inflate drug prices or to private healthcare organizations, who then exploit data to improve their own competitive advantage and thus refuse to share it, despite this being in the best interest of patients, clinical research or insurance claims (Winter and Davidson 2017). To facilitate value realization while balancing conflicting stakeholder interests and needs, data ventures can emerge across the organizational boundaries of hospitals, clinics, urgent care centers or other healthcare organizations to devise appropriate data governance. Instead of attempting to restrict wide-scale health data mining to avoid ethical issues or conflicting interests (Winter et al. 2019), data ventures can provide the necessary intermediate localities for negotiating working compromises between competing concerns as they become salient.

Traditional approaches to data governance encourage the empirical study of formal structures, roles, loci of decision making, principles and the like. Evidence from research and practice alike suggests data use in organizational practice will be characterized by multiple competing concerns, which make stable arrangements volatile. As an alternative, the notion of a data venture provides an integrative understanding and a basis for managing how data governance is spontaneously formed, adapted and evolved through temporary self-rising, organizational arenas. Despite limited resources, low goal alignment and diverging stakeholder interests, data ventures absorb major risks associated with data use as they emerge to develop local resolutions for competing concerns. What makes data ventures capable of spontaneous organizing and unstructured problem-solving, also makes them difficult to manage with established data governance approaches in traditional bureaucracies. The next and final section will revisit key assumptions and propose a broader conceptualization of data governance.

2.4. RETHINKING KEY ASSUMPTIONS OF DATA GOVERNANCE

While extant literature is heavily skewed toward top-down approaches to strategic data asset governance involving managerial tasks of determining data principles, decision-making rights and responsibilities, emerging research indicate data governance also encompasses a multitude of informal organizational activities involving the arranging,

curation and use and of data in everyday work practices. Governing data involves interweaving managerial decisions about the overarching direction for data use with improvised operational choices for how to appropriate specific data sets, when performing work under local conditions, restraints and opportunities. It involves enmeshing social processes of strategizing, coordinating, communicating and interpreting in data-related activities with numerous technical practices such as processing low-fidelity spreadsheets, implementing cybersecurity protocols, changing technical IT infrastructure, developing algorithms or otherwise producing and amending the material arrangements of data (Dourish 2017). To accommodate the breadth of these activities, this dissertation adopts an understanding of data governance as *a fast-growing, constantly changing set of digital practices involved in the organizing of data use*.

As diverging assumptions for data use across these activities also begin to manifest as conflict in practice, data ventures can unfold and be brought to bear in self-rising, temporary organizational arenas, where appropriate data governance arrangements can be improvised. Traditional data governance models rely heavily on compartmentalization and hierarchical designation of authority and control for data-related activities, but when governance outcomes depend on distributed knowledge in locally situated, autonomous units, like data ventures, "control can no longer be focused on … adherence to behavioural prescriptions passed down a hierarchy" (Child and Rodrigues 2003, p. 344). As data ventures claim advantages in terms of improvised negotiation and local decision-making, they simultaneously present new challenges for governance and control.

Data ventures do not replace hierarchy and routine, for example in conventional areas of work, where consistency and efficiency are dominant (Kellogg et al. 2006), but organizations that rely on multiple, fluid centers of expertise (Neff and Stark 2004) and temporary agreements (Girard and Stark 2002) require more responsive approaches to governance. Previous research in IT governance has experimented with hybrid federalism as a way to balance centralized standardization with decentralized flexibility (Brown 1999; Weill 2004; Williams and Karahanna 2013), but such structures still rely on output controlled coordination mechanisms, which are difficult to define and expect under conditions of rapid change and high uncertainty (Sabel and Zeitlin 2012), as is characterized by the way data ventures spontaneously emerge and dissolve.

In this vein, Sambamurthy and Zmud (2000) challenged the fundamental assumption that governance should necessarily be about organizational structure and design. They proposed instead the concept of an *organizing logic* as "the managerial rationale for designing and evolving specific organizational arrangements in response to an enterprise's environmental and strategic imperatives" (Sambamurthy and Zmud 2000, p. 107). Much like data governance, traditional IT governance with its formal structures, governance modes and loci of decision making (Brown and Grant 2005) were pressured by growing demands for scalability, flexibility and quick adoption of emerging technologies in the emerging digital economy. Rather than pursuing business goals of growth, scale or efficiency through prescriptive governance architectures like, centralized,

decentralized and federal, IT leaders should instead adopt an organizing logic for their enterprise's IT activities focused on developing core IT capabilities, which could be assembled, distributed, or reassembled through various integration architectures in response to emerging challenges and opportunities from the business environment (Sambamurthy and Zmud 2000, p. 111).

In a similar vein, this dissertation seeks to advance knowledge on data governance by theorizing a corresponding organizing logic which enables organizations to devise appropriate organizational arrangements that support the fast-growing, constantly changing set of digital practices involved in data use. Such an organizing logic must necessarily attend to inherent diversity, uncertainty and equivocality; to accommodate multiple planned and improvised data-related activities, of strategic, operational, social and material character, and the responsive negotiation of competing concerns between them, as they arise in practice. Against this backdrop, the next chapter explores *polycentricity* to theorize an organizing logic for data governance in the digital era.

CHAPTER 3. THEORETICAL FRAMING

3.1. EXPLORING POLYCENTRICITY AS AN ORGANIZING LOGIC

To theorize how organizations can balance planned and improvised data-related activities and devise appropriate organizational arrangements supporting the fast-growing, constantly changing set of digital practices involved in data use, this dissertation turns to the concept of *polycentricity* (Ostrom 1990).

Originally, polycentricity was conceived by Polanyi (1951) to characterize the juxtaposition between rigor of the scientific method and freedom of expression in the social organization of science. In a broader sense, polycentricity may be defined as "a social system of many decision centers having limited and autonomous prerogatives and operating under an overarching set of rules" (Aligica and Tarko 2012, p. 237). Polycentricity resembles the logic of complete decentralization in a monocentric system, but a key difference remains. In a polycentric system, there is no central authority to designate and coordinate decision-making; only spontaneous emergence of self-rising individual decision-making centers that are formally independent, but make mutual arrangements to take each other into account (Ostrom et al. 1961). In the social organization of science, this means that individual researchers are free to pursue their own research agendas across a near limitless number of topics, but remain exceedingly loyal to established research fields, methods, traditions, quality criteria, philosophies, etc. As researchers continuously instantiate their own work within larger bodies of knowledge, they contribute to overall, metalevel scientific progress (Aligica and Tarko 2012; Polanyi 1951; Suddaby 2010). No central, coordinating authority determines where researchers direct their attention, but ongoing activities in surrounding decision-making centers are inevitably shaping decisions, for example in response to calls for specific publications in prestigious research outlets, available research grants, enduring scientific issues, prevalent societal challenges, and many more.

As an organizing logic, polycentricity is essentially characterized by individual, self-rising, autonomous elements mutually adjusting to create orderly relationships with each other within a larger system of rules (Ostrom et al. 1961). Polycentric governance has been explored by scholars in political science (Aligica and Tarko 2012), public administration (McGinnis and Ostrom 2012; E. Ostrom 1972; Ostrom et al. 1961), and policymaking (Carlisle and Gruby 2017), as a radical alternative to centralized public service distribution. The most influential work however was done by Elinor Ostrom (1990) in her study of governance in long-enduring, self-organizing, natural resource systems and also forms the basis for the theoretical framing in this dissertation. The following section details key features of polycentric governance in self-organizing resource systems, drawing on Ostrom's ideas as well as extant IS literature, while the final section outlines how an organizing logic of polycentricity can be studied for data governance.

3.2. POLYCENTRIC GOVERNANCE IN SELF-ORGANIZING RESOURCE SYSTEMS

In her original empirical studies of numerous fisheries, irrigation developments water basins and forestries, Ostrom (1990, p. 29) set out to address how a group of individuals in an interdependent situation can organize and govern themselves to obtain join benefits when they all face temptations to act opportunistically. Ostrom originally studied self-organizing of natural common pool resources (CPRs), in which various threats, such as overuse, pollution and free-riding, jeopardize the long-term viability of the system, and where a high degree of openness and accessibility render exclusion of anyone not contributing to maintenance and provision of the resource unfeasible. A group of appropriators[4] remain interdependent given their mutual reliance on the CPR as a source of economic activity, but face substantial issues in adopting coordinated strategies for how to govern this collective resource:

> "the problem facing CPR appropriators is one of organizing: how to change the situation from one in which appropriators act independently to one in which they adopt coordinated strategies to obtain higher joint benefits or reduce their joint harm. That does not necessarily mean creating an organization. Organizing is a process" (Ostrom 1990, p. 39)

Hardin (1968) had previously conceived *The Tragedy of the Commons,* positing that individuals with access to a common pool of resources would continue to unsustainably exploit the resources, until the system collapsed, unless governing measures were implemented by a coercive, central "power" (Hardin 1968; Holahan and Lubell 2016; Ostrom 1990). At the time, dominant theories of market and state could not explain how some communities in natural resource systems as observed by Ostrom still managed to overcome complex issues and supply and sustain effective, intricate institutions of norms and rules for governing their collective resource over time, despite not behaving as markets or states.

Upon reviewing the commonalities between governance in long-enduring natural resources, Ostrom found there was no single set of rules optimal for dealing with specific and general problems experienced by appropriators, but rather a series of principles characterizing the designs of robust self-organizing (detailed later in section 3.2.4). At the core, such systems organize governance to increase opportunities for adaption and

[4] Ostrom identified three distinct stakeholder categories in a self-organizing resource system; *producers* who constructs, repairs, or takes actions to ensure the resource system itself; *providers* who arrange for provision of the resource and *appropriators* who withdraw resource (units) from the system (Ostrom 1990 pp. 30-31)

learning in the face of change and uncertainty by progressively defining, adapting, and enforcing rules to fit local conditions, with self-correcting mechanisms for monitoring and sanctioning compliance with rules (Ostrom 1990, 2005). Over time, threats from within and outside the environment inevitably emerge and challenge existing governance arrangements, but intricate nesting of rules and action arenas allow appropriators to spontaneously address and resolve concerns with considerable independence and autonomy.

In this vein, several core features of polycentric governance in self-organizing resource systems represent viable options enabling organizations to devise appropriate organizational arrangements that support the fast-growing, constantly changing set of digital practices involved in data use. Governing data in organizations involve similar considerations of how to arrange the provision of data as a collective resource; achieve robustness under conditions of uncertainty and local autonomy; mobilize individuals with little incentive to organize; and, enact governance in practice. These are detailed in the following.

3.2.1. ARRANGING PROVISION OF A COLLECTIVE RESOURCE

Original work concentrated on specific problems associated with provision of physical, tangible resources, such as fish, timber, water and soil, with high degrees of accessibility, openness and depletion (Hardin 1968; Ostrom 1990). Since depletable means consumption of a resource by one individual prevents another from consuming the same resource, conceptual foundations may initially appear inconsistent, since digital data can be used by many individuals at the same time and copied nearly infinitely with negligible extra cost (McKinney and Yoos 2010). Both Ostrom and other researchers have, however, convincingly applied polycentricity as theoretical frame to study self-organized provision of other collective, intangible resources, including academic knowledge (Hess and Ostrom 2007), online, distributed information commons (Mindel et al. 2018), information infrastructures (Constantinides and Barrett 2015; Vassilakopoulou et al. 2018) and genome health data (Skorve et al. 2017; Vassilakopoulou et al. 2019).

Many differences persist between natural resources and organizational data. Yet, Mindel et al. (2018) theorized distributed, online information systems, like Wikipedia, Yelp, Twitter, YouTube, Github etc, as information commons subject to multiple issues of information congestion, pollution, violation and rebellion which threaten continued vitalization and appropriation of information in these online systems over time. Authors found that "although digital information is vastly different from physical resources … information commons are nonetheless susceptible to … threats traditionally more associated with physical systems" (Mindel et al. 2018, p. 624) thus depend on polycentric governance practices enacted by their distributed userbases.

Moreover, it is worth noting that data governance involves producing and amending material arrangements of data (Dourish 2017) in various forms, despite general notions

of data as abstract and intangible. Among multiple understandings of data, a token view asserts that information acquires tangibility when encoded and processed as data in information systems, where it can then be stored, shared, retrieved, manipulated and distributed (McKinney and Yoos 2010; Mindel et al. 2018). When a practitioner in an organization records enumerated data items in a spreadsheet, manipulates them through functions and formula, saves and forwards the file by e-mail to a colleague, they are essentially engaging in appropriation activities of a collective resource comparable to fishermen trawling fresh-water minnows in an inshore fishery. Such activities are nonetheless governable and can be subjected to rules through data governance arrangements.

Data as a collective resource in organizations are not open but unfold within some type of enforceable boundaries. In this sense, data governance does not share identical concerns for overcoming problems of openness, accessibility and free-riding like the self-organizing resource systems studied by Ostrom (1990) and Mindel (2018). It does however share similar concerns about how to overcome inherent problems faced by a group of individuals looking to organize provision of a collective resource, despite heterogenous interests and ideologies. Unlike open-access commons, traditional organizations can rely on formal hierarchy and authority to install behavioral and outcome controls that impose governance (Child and Rodrigues 2003). Such mechanisms are predominant in existing data governance research (Abraham et al. 2019) but limited in apprehending the multitude of operational activities involved in organizing data (Benfeldt et al. 2020; Parmiggiani and Grisot 2020). Emphasizing top-down control may alienate practitioners (Constantinides and Barrett 2015) and result in conflicts or break downs in the everyday governance practices of collective resources (Boonstra et al. 2017), even within organizational boundaries.

Similar to other self-organizing resource systems, arranging for the provision of data as a collective resource within an organization thus involves incentivizing a group of individuals with heterogenous interests and perspectives to adopt coordinating strategies for how they appropriate data in their local work practices. Individual departments depend on, produce and appropriate data in multiple, overlapping ways to oversee their day-to-day responsibilities and may not readily wish to abide by general arrangements for data governance imposed by management. Enacting polycentric governance can help to overcome this problem of organizing.

3.2.2. ROBUSTNESS IN SELF-ORGANIZING RESOURCE SYSTEMS

Self-organizing resource systems can be considered robust if they manage to devise, modify and adapt governance arrangements over time to maintain desired system characteristics despite fluctuations within and outside its environment (Ostrom 2005). Much to her frustration, Ostrom was not able to identify a prototypical set of rules (institutions) associated with robustness in her original work and ultimately conceived instead on a series of design principles, detailed later in section 3.2.4. Ostrom did however

conceive two central components of self-organizing a resource system; the nesting of rules at multiple levels, and the use of action arenas to shift between levels and devise governance in layers.

Ostrom conceived three levels of rules cumulatively affecting how individuals can appropriate resources in the system (Ostrom 2005, 1990). *Operational rules* govern the day-to-day decisions made by individuals that involves storing, sharing, retrieving, manipulating, distributing or otherwise processing data enmeshed in a wealth of other deliberate and improvised activities. This includes both de facto and de jure rules specifying how individuals can act in the system (Mindel et al. 2018) *Collective-choice rules* govern how appropriators, authorities or other actors make arrangements for how a resource should be managed – the operational rules – in everyday activities of the system. Such rules specify whom in what positions can make rules about what in which way given what information, benefits and costs (Ostrom 2005). Finally, *constitutional rules* govern foundational aspects of how organizing in the resource system works, including who can participate, rules for changing arrangements (collective-choice) and core system characteristics (Ostrom 1990, 2005). Constitutional rules provide fundamental expectations of behavior from individuals, so when they are changed, which happens very rarely, it introduces significant uncertainty and instability in existing governance arrangements (Ostrom 2005). Data-related activities in everyday organizational work occurs at operational level; decisions about how data may be appropriated in such various activities occur at collective-choice level, while underlying expectations and norms for acceptable conduct are formed at constitutional level.

Individuals in self-organizing resource systems shift between these levels to solve problems experienced in the empirical, organizational setting by employing different *action arenas*. (Ostrom 1990). Action arenas involves situations, where particular types of actions can occur:

> "an action situation refers to the social space where participants with diverse preferences interact, exchange goods and services, solve problems, dominate one another, or fight (among the many things that individuals do in action arenas)." (Ostrom 2005, p. 14)

Action arenas can be formal, like boards, committees, courts and legislative bodies, or informal, like meetings, conversations and brief encounters in an organization (Ostrom 1990). When incongruities, threats, conflicts or other tensions emerge in operational situations, individuals can either adopt a different strategy for coping within current conditions or seek to change the rules, by engaging action arenas at constitutional and collective-choice levels. Frequently, several collective-choice arenas affect the operational rules used in practice and thus represent various opportunities for affecting rule change. Subsequently, collective-choice arenas enable practitioners in self-organizing resource system to engage in both strategic, managerial and operational decision-making for how resources may be appropriated in the organization. Decisions-making rights, decision domains and responsibilities are not necessarily designated *a priori* through formal roles

but enacted in specific action situations that arise when individuals seek to deal with a prominent issue.

Nesting rules in this manner is what allows self-organizing resource systems to adapt and remain robust over time in the face of conflict. In their study on the formation of a regional health information infrastructure, Constantinides and Barrett (2015) detail how local users, developers and government principals attribute different meanings to the infrastructure based on their ideological positions, shaping relations of power and legitimacy and triggering resistance to any imposed governance arrangements challenging their own position. The infrastructure involved primary care centers, regional government officials and national government, effectively interlacing three stakeholder groups with their own set of operational, collective-choice and constitutional rules into a meta-constitutional level (Ostrom 2005) of expectations for how individuals need to contribute to the infrastructure. Centralized, top-down approaches for defining and enforcing rules would inevitably yield resistance, so rules were progressively nested instead:

> "A higher layer assists lower-layer stakeholders (e.g., general practitioners in primary care centers) … to the extent that they trust the higher layer (e.g., the Regional Health Authorities) not to fail them. Similarly, lower-layer stakeholders should be free to govern themselves as long as their self-governance does not affect others in the same or higher layers. Hence, governance is nested to higher layers until a layer is reached where all individuals with a substantive interest … are represented adequately." (Constantinides and Barrett 2015, p. 14)

Stakeholder groups self-organize to the point it causes spillover effects on other group interests and only then is governance "nested to a higher level" through negotiation of the appropriate arrangement in a collective-choice arena, which can affect the problematic operational situation.

Rapid change in, for example national court decisions about rules concerning all resources of a particular type, relative importance of the resource in its broader environment, advances in technology and heterogeneity of individuals remain sources of potential disruption in systems that have:

> "adapted an effective way of coping with a particular technological, economic, or social environment …. to adjust to slow changes in one or several variables if substantial feedback is provided about the consequences of these changes for the long-term sustainability of the resource and/or the set of institutions used for governing that resource" (Ostrom 2005, p. 272)

Extensive change in multiple conditions, either within or outside the resource environment put pressure on individuals to cope with new conditions. Self-organizing resource systems are inherently subject to threats caused by tensions between individual-

level actions and collective interests (Hardin 1968; Mindel et al. 2018; Ostrom 1990) but as incongruities or conflicts emerge in practice, individuals can negotiate new rules for coping with the specific threats in dedicated collective-choice action arenas. As determined by Ostrom (1990, 2005) self-organizing resource systems remain robust because they evolve and adapt rules in response to emerging threats over time, resulting in a nested set of rules tailored to the specific conditions inherent to the system.

Action arenas constitute a focal unit of analysis in the polycentric governance of self-organizing resource systems (Ostrom 2005). Actions taking place to amend operational, collective-choice and (very rarely) constitutional rules cannot meaningfully be studied as processes occurring at separate levels of analysis (Ostrom 1990, 2005). Instead, zooming in and zooming out constitute useful perspectives to understand and explain how institutional change unfolds across levels (Nielsen et al 2014). Scholars looking to examine polycentric governance in self-organizing resource systems can switch between zooming in; observing how participants interact, address problem-solving, and devise rules in specific action arenas and; and zooming out to consider the exogenous conditions shaping an action arena or how action arenas are linked to others (Ostrom 2005, p. 15). Traditional distinctions between strategic, managerial and operational behaviors for data governance (Alhassan 2019) do not occur as separate, asynchronous activities at different hierarchical levels in self-organizing resource systems but simultaneously within specific action arenas that can be zoomed in on. In polycentric governance, making, changing and enacting rules are interwoven processes; not separate feats of designing a set of rules, planning their roll-out and then implementing them through change management.

3.2.3. SUSTAINING VERSUS MOBILIZING COLLECTIVE ACTION

The structure of incentives facing a group of individuals are consequential, both for sustaining and mobilizing collective action in polycentric governance. Early rational models of human behavior assumed individuals in a group sharing a common overall objective would naturally engage in collective action (Holahan and Lubell 2016). Olson (1965) first challenged this proposition by conceiving the free-rider problem; individuals who benefit from a resource, will not voluntarily contribute to its production (Olson 1965; E. Ostrom 1990) and then Hardin (1968), who propositioned resource systems will inevitably collapse due to individual opportunism, unless governed by a coercive, central power. Governance for collective action is about incentivizing cooperation by redefining individual payoffs through a combination of top-down mandates and bottom-up self-organizing (Holahan and Lubell 2016, p. 21) to reduce the provenance of harmful, individual-level actions which, when aggregated, threaten the survival of a resource system. Structuring incentives appropriately can mobilize collective action by re-orienting a group to adopt coordinated strategies, which produces overall better results for everyone than if they acted individually (Ostrom 1990)

Empirical studies indicate mobilizing collective action for data governance is difficult (see section 2.2), specifically because individuals in organizations have weak incentives for

adopting coordinated strategies for governing data as a collective resource (Benfeldt et al 2020). As earlier in the previous section, designing and implementing rules for appropriation of data are seen as two separate activities (Alhassan 2019), where the former depends on assumptions of rational decision-making and the latter on reflexive change management (Vilminko-Heikkinen and Pekkola 2019) In effect, supplying new institutions – sets of rules across operational, collective-choice and constitutional levels – for data governance in one major, transformational step by defining overall, abstract rules for organizing data (Khatri and Brown 2010) and systematically rolling out (Ladley 2012) do little to incentivize cooperation. In self-organizing resource systems, mobilizing and sustaining collective action are not seen as fundamentally different problems; while the structure of incentives differ, both essentially involve progressively affecting small-scale change (Ostrom 1990).

As mentioned earlier, robust self-organizing resource systems sustain collective action for polycentric governance by facilitating adaption and learning, and progressively devising layered rules in action arenas arising in response to specific threats. Similarly, mobilizing collective action involves re-incentivizing individual-level actions towards adopting coordinated strategies, which may be achieved by addressing second and third-order problems (Ostrom 1990). Rather than immediately devising complex, large-scale governance arrangements, mobilizing collective action for polycentric governance involves gradually restructuring incentives by addressing smaller parts of a large-scale problem, with local, low-cost resolutions that demonstrate early success and high benefits to individuals (Ostrom 1990, p. 141). Besides offering information about problems facing individuals, each little change alters the overall structure of incentives within which future, strategic decisions are to be made. Establishing polycentric governance for a resource system is not about beginning from scratch, or taking one large step, but about progressively transforming existing multiple status quos (Ostrom 1990, 2005)

By extension, bounded rule making is central to self-organizing resource systems. While experimentation is fundamental to small-scale governance arrangements, they are not directly comparable to traditional experiments or cross-functional projects in organizations (Kellogg 2006). Small-scale governance arrangements involve collective action within a bounded group of appropriators, who devise rules for their specific area of the resource system, leveraging deep contextual knowledge about the local conditions and by fostering shared norms of reciprocity and close social ties (Ostrom 1990). Appropriators frequently interacting in other situations are apt to develop and enforce effective rules and norms for acceptable behavior, because they, through their frequent interactions, can convey mutual expectations and observe compliance in reinforcing encounters (Ostrom 1990 p 206). Benefits gained from small-scale, incremental, self-transforming arrangements can create momentum for devising larger arrangements:

> "Success in starting small-scale initial institutions enables a group of individuals to build on the social capital thus created to solve larger problems

> with larger and more complex institutional arrangements [through] the process of accretion of institutional capital" (Ostrom 1990 p 190)

Mobilizing collective action among smaller groups of individuals also reduces the impact of diverging heterogenous interests (Constantinides and Barrett 2015), while accumulating social and institutional capital to eventually tackle complex issues. Allowing situated decisions about the best rules for governing the resource under specific local conditions offers a wide range of benefits. Just like constitutional rules provide a general set of rules within which individuals can organize operational and collective-choice rules, small-scale arrangements need large-scale supportive institutions to provide reliable information about conditions in the resource system. As noted earlier by Constantinides and Barrett (2015), the presence of large-scale institutions may have preemptive effects on conflict-resolution mechanisms, since local individuals know they can rely on assistance and order in some form from outside the small-scale arrangement. Smaller arrangements are allowed to devise rules for their bounded area of the resource system, until activity, condition, rules or conflict require input from others or large-scale institutions (Constantinides and Barrett 2015; Ostrom 1990).

3.2.4. DESIGN CHARACTERISTICS OF ROBUST, SELF-ORGANIZING RESOURCE SYSTEMS

Much to her dismay, Ostrom analyzed a wide variety of robust, self-organizing systems, but she could not identify any commonalities among their operational and collective-choice rules:

> "It was frustrating that I could not identify any particular rules consistently associated with robust governance of common-pool resources. Instead of focusing on specific rules, my effort turned to identifying eight underlying design principles that characterized robust … institutions. No assertion was made that those crafting these institutions self-consciously used the design principles." (Ostrom 2005, pp. 258-259)

Despite significant in-depth, empirical inquiry, no two forestries, irrigation developments, water basins or fisheries were seen to apply the same rules; their arrangements were not determined by the resource either, but instead by contextual conditions and historical developments. Thus, Ostrom instead conceived eight principles characterizing the design of robust, self-organizing resource systems (see Table 5) that manage to remain sustainable in the long term. Design principles do not imply that individuals deliberately applied the principles in establishing governance, but rather that robust systems exhibit these characteristics to a larger extent, while collapsing or underperforming systems do not or to a lesser extent.

#	Design principle	Explanation
1	Clearly defined boundaries	Individuals or households who have rights to withdraw resource units from the CPR must be clearly defined as must the boundaries of the CPR itself
2	Congruence between appropriation and provision rules and local conditions	Appropriation rules restricting time, place, technology and/or quantity of resource units are related to local conditions and to provision rules requiring labour, material and/or money
3	Collective choice arrangements	Most individuals affected by the operational rules can participate in modifying the operational rules
4	Monitoring	Monitors, who actively audit CPR conditions and appropriator behaviour are accountable to the appropriators or are the appropriators
5	Graduated sanctions	Appropriators who violate operational rules are likely to be assessed graduated sanctions (depending on the seriousness and context of the offense) by other appropriators, by officials accountable to these appropriators or by both
6	Conflict-resolution mechanisms	Appropriators and their officials have rapid access to low-cost local arenas to resolve conflicts among appropriators or between appropriators and officials
7	Minimal recognition of rights to organize	The rights of appropriators to devise their own institutions are not challenges by external governmental authorities
8	Nested enterprises	Appropriation, provision, monitoring, enforcement, conflict resolution and governance activities are organized in multiple layers of nested enterprises

Table 5. Design principles illustrated in sustainable, self-organizing resource systems (adapted from Ostrom 1990 p. 90)

An important design principle is establishing the boundaries of the resource system (Design principle #1); it enables participants to know who is included in a set of relationships and whom to cooperate with (Ostrom 2005, p. 261). Such boundaries may be marked by well-understood attributes of members, such as working in a specific department or with a specific domain, or through specific social customs which signify

to others that individuals can be trusted. Boundaries imposed by external authorities are unlikely to be recognized by individuals, especially if they have cared for the resource prior. Thus, merely defining boundaries is not sufficient in itself; they have to be continuously enacted by individuals who know that they have mutual responsibilities and benefits in regulating these boundaries of their collective resource.

According to Ostrom (1990, p. 93), local experimentation and resilience remain successful because "individuals who directly interact … with the physical world can modify the rules over time so as to better fit them to the specific characteristics of their setting". Self-organizing resource systems adapt by employing specific social mechanisms, in which rules governing how individuals may appropriate resources are both proportionally equivalent with the local conditions of the empirical setting (Design principle #2) and devised through collective-choice arrangements, where individuals affected by the rules can participate in making and modifying them (Design principle #3). Processes for crafting rules are complex, but more likely to yield effective outcomes, if they are based on existing rights and reflect local norms and values of individuals (Ostrom 2005, p. 264).

Because there is no all-knowing, central authority to enforce agreements, polycentric governance arrangements require their own internal enforcements to ensure commitment and deter rule-breakers (Ostrom 1990). In self-organizing resource systems, this is mutually achieved through peer-monitoring (Design principle #4) and graduated sanctions (Design principle #5). Ostrom notes that most long-enduring regimes create official positions for monitors, who then keep track of conditions for and individuals engaging in appropriation activities (Ostrom 2005, p. 265). If a monitor discovers rule-breaking, rules in self-organizing resource systems are often designed in a way such as to have virtually *no* sanctions upon the first violation (Ostrom 1990, 2005). Rather, a low-impact initial sanction is seen as providing information to the individual that everyone can make a mistake, but their infraction has been noticed. Local individuals are more likely to identify rule breakers long before any external monitors (Bennett et al. 2009), because they are actively involved in shaping rules and therefore motivated to monitor rule-breakers as a "by-product of their own motivations" (Ostrom 1990, p. 95) to engage in governance of the resource system. In sum:

> "When the users of a resource design their own rules that are enforced by local users … using graduated sanctions … that clearly define who has rights to withdraw from a well-defined resource … and that effectively assign costs proportionate to benefits …, collective action and monitoring problems tend to be solved in a reinforcing manner" (Ostrom 2005, p. 267)

In polycentric governance, no central, all-knowing authority can ensure rules are adhered to. Cheap, local mechanisms for discussing and resolving what constitutes rule-breaking or suboptimal rules are therefore critical to sustain collective participation in governance arrangements (Design principles #6). If these mechanisms are well-known to be effective among individuals, the overall number of conflicts are likely to reduce, since all parties

are aware issues can be escalated if need be (Ostrom 2005, p. 268). Mindel et al. (2018) exemplify peer-monitoring, graduated sanctions and low-cost conflict resolution in information commons, where users often have the option to report illicit behavior to administrators, who can then issue a first warning to the infractor and ultimately block their access, if violation escalates.

Though their right to self-organize is not contested by external authorities (Design principle #7), polycentric governance activities in larger, more complex forms of resource systems are often nested in multiple layers within themselves and with other local, regional or national government jurisdictions (Design principle #8) (Ostrom 1990). As noted multiple times, nesting is a key feature of robust governance, because it helps overcome the problems associated with relying only on large-scale or small-scale governance arrangements. Social norms, trust, expectations of reciprocity and deep contextual knowledge can only be achieved close to empirical settings on a small scale, while general expectations of behavior, scientific knowledge, technological advancements and official settlement of disputes require supportive, large-scale institutions. Enmeshing these activities in layers can allow individuals enough autonomy to deal with spontaneous disturbances in the system, while still maintaining some structured order of relationships, as exemplified in the formation of a regional information infrastructure involving both operational rules for general practitioners in primary care centers and official governance by government principals (Constantinides and Barrett 2015).

Finally, polycentricity is an abstract organizing logic underlying how governance is evolved and enacted in self-organizing resource systems. Ostrom (2005, p. 270) warns against using the design principles as blueprints for building the "right" organizational design to govern a resource, while Mindel et al. (2018) indicate sustainable information commons integrate polycentric governance in their design by engaging in a series of polycentric governance practices. The final section in this chapter will elaborate how the abstract notion of polycentric governance can be studied for data governance.

3.3. STUDYING AN ORGANIZING LOGIC OF POLYCENTRICITY FOR DATA GOVERNANCE

As mentioned in section 2.4, an organizing logic for data governance in the digital era must necessarily attend to inherent diversity, uncertainty and equivocality. Data governance involves both deliberate and emergent organizing of data-related activities, where a constantly changing set of managerial, operational, social and digital practices interweave, and result in multiple competing concerns for data use. Insights from literature on governance in self-organizing resource systems indicate polycentricity is an underlying organizing logic which enables individuals to progressively adapt and develop robust, congruent sets of rules and thus constitutes appropriate for attending to key implications for data governance in the digital era.

Polycentric governance assumes the use of multiple, different action arenas, formal, informal, spontaneous, and deliberate, where individuals can devise appropriate rules in response to emerging problems from within and outside the resource system. Individuals ultimately affected by these rules are able to actively participate in their formation and ensure they remain congruent with local conditions.

Rather than conceptualizing governance as the separate, chronological activities of first designing and then implementing rules and responsibilities for data governance, an organizing logic of polycentricity instead depend on a multitude of action arenas; situations, where particular types of action can occur and multiple managerial, operational, social and digital practices are leveraged in combination to negotiate competing concerns and devise appropriate data governance arrangements. Such arrangements can also include formal rules and responsibilities for data but are just as likely to involve amendments to local work routines, new collaborations, various technical solutions or similar outcomes.

Themes from existing literature on polycentric governance in self-organizing resource systems, as detailed in this section, thus form the basis for the later generation and analysis of empirical material (see Chapter 4). As elaborated later (see section 4.1.3.2), theorizing in this study is not concerned with testing propositions but with developing novel theoretical ideas that are useful for researchers in coping with, reasoning about and further investigating the many, multifaceted issues implicated in the fast-growing, constantly changing set of digital practices involved in the organizing of data. The broad themes used to conceptualize an organizing logic of polycentricity for studying data governance (summarized in Table 6 by the end of this section) should therefore not be seen as "constructs [or] small buckets narrowly defined" but rather as "large buckets or broad concepts loosely defined" (Suddaby 2010, p. 354).

The research question (see section 1.5) not only directs attention to how polycentricity enables organizations to devise data governance, but also how it evolves to do so. What is emphasized in the empirical case is therefore not a complete analysis of ongoing polycentric governance, but rather the incremental, sequential, self-transforming changes in the organization which eventually emerge in continuous organizing patterns (V. Ostrom 1972) of polycentric governance (see Chapter 6). In her original empirical work on self-organizing resource systems, Ostrom (1990) notes that studying the origins of robust governance arrangements involves addressing a different set of issues, such as:

> "How many participants were involved? What was their internal group structure? Who initiated action? Who paid the costs of entrepreneurial activities? What kind of information did participants have about their situation? What were the risks and exposures of various participants? What broader institutions did participants use in establishing new rules? These questions are rarely answered in the extensive case-study literature describing behavior within ongoing institutional arrangements. Once a set of rules is in

> place, the incentives facing appropriators are entirely different from the incentives that faced an earlier set of appropriators" (Ostrom 1990, pp. 103–104)

Essentially, an organizing logic of polycentricity is an abstract notion that manifests in the rules and characteristics of a self-organizing resource system as well as the way in which individuals enact organizing patterns (V. Ostrom 1972). As the empirical analysis undertaken in Chapter 5 is informed by themes from extant literature, it deals just as much with the questions outlined by Ostrom, by observing focal actors, prominent threats to collective action, how actors learn about threats as well as the boundaries of the resource system, how incentives change and shape collective action and which action arenas are involved to establish rules.

Themes	Explanation	Sources	Questions for the empirical analysis
Data as a collective resource	Data is perceived as a resource by individual practitioners, both as a general idea and in specific instance, by acknowledging the value of adapting prior individual-level actions in favor of new data governance arrangements because it ultimately provides higher benefits	Ostrom (1990, 2005) Constantinides and Barrett (2015)	How do individuals relate to costs and benefits involved in data as a collective resource? What were the entrepreneurial costs to arrange for data as a collective resource, ie. informal relationship building, social capital, obtaining information?
Collective action threats	Emerging issues, conflicts, contradictions or tensions between individual and community-level interests for data use emerging in practice, with potential to undermine participation in data governance arrangements	Ostrom (1990, 2005) Mindel et al. (2018)	What were the problems to be overcome in evolving data governance? Who was exposed to risks?
Polycentric governance	Actions, activities or other organizing patterns taken by individual practitioners which reflect the eight principles characterizing robust self-organizing systems	Ostrom (1990, 2005) Mindel et al. (2018)	How are the design principles enacted in practice? How are they observed? Who enacts them?
Focal actors	Individual practitioners engaging in actions or activities associated with polycentric governance or otherwise advances evolution of data governance arrangements	Ostrom (1990, 2005) Constantinides and Barrett (2015) Nielsen et al. (2014)	Who were the central practitioners? Who initiated actions? Who paid the entrepreneurial costs ie. informal relationship building, social capital, getting information?
Action arenas	Specific formal, informal, spontaneous or planned situations where individual practitioners solve problems related to data use and/or make new rules for data governance, which result in outcomes for the organization	Ostrom (1990, 2005) Constantinides and Barrett (2015) Nielsen et al. (2014)	Which types of action are afforded in which arenas? Where are actions to organize taken?
Sequence of actions	The instantiation of specific actions or activities by individual practitioners at a given time throughout the process of evolving polycentric governance	Ostrom (1990, 2005)	When were specific actions taken to overcome threats to collective action? Who took action?
Involvement of existing institutions	The influence of existing structures, rules, processes, relationships or other organizing patterns within or outside the organization in devising data governance arrangements	Ostrom (1990, 2005) Constantinides and Barrett (2015) Nielsen et al. (2014)	What existing structures, processes, relationships for organizing were used? How were small and large-scale institutions within and outside the organization involved in structuring incentives and practicing rule-making?

Table 6. Studying polycentricity in data governance

CHAPTER 4. RESEARCH APPROACH

4.1. RESEARCH DESIGN

In the pursuit to advance knowledge on data governance both as a topic of theoretical interest and a collection of key issues experienced by practitioners, this dissertation adopts an engaged scholarship approach (Van de Ven 2007). At its core, engaged scholarship actively seeks to bridge a theory-practice gap (Kieser and Leiner 2009) by affording researchers the opportunity to contribute with rigorous theoretical development, while still addressing relevant, real-world problems anchored in practice (Mathiassen 2017).

What makes engaged scholarship "engaged" is the anchoring of research in a real-world problem situation as experienced by key stakeholders (Mathiassen 2017). Most real-world problems do not respect the boundaries of professional domains and often exceed the capabilities of individuals to address them alone. By actively involving various stakeholders and exploiting their specialized knowledge backgrounds, both theoretical and practical insights are likely to be more penetrating and insightful (Van de Ven 2007). Different models for engagement and attachment are available, depending on the overarching research objective (see Figure 2).

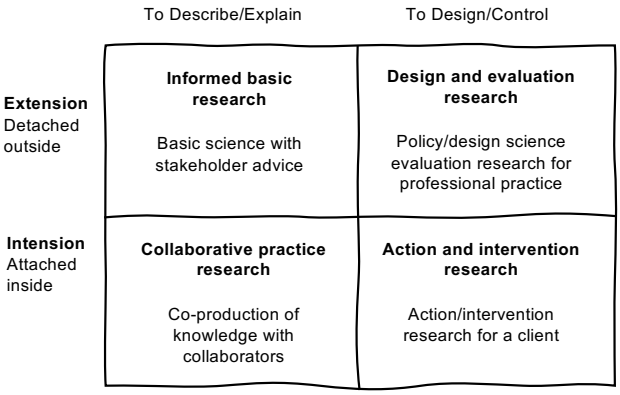

Figure 2. Forms of engaged scholarship (reproduced from Van de Ven, 2007)

For purposes of describing or explaining sociotechnical phenomena, researchers can either approach questions detached from the outside with input from stakeholders, or attached inside, co-producing knowledge with collaborators (Van de Ven 2007). This dissertation adopts a collaborative practice form of engagement, which is well-suited for

co-producing basic knowledge about a complex problem or phenomenon (Mathiassen 2002; Mathiassen et al. 2012; Van de Ven 2007) and fits well with the dedication of this dissertation to study the emergence and development of a specific, contemporary phenomenon. Foundational to collaborative practice research is that:

> "Instead of viewing organizations and clients as data collection sites (…), an engaged scholar views them as a learning workplace (…), where practitioners and scholars co-produce knowledge on important questions and issues by testing alternative ideas and different views of a common problem." (Van de Ven 2007, p. 7)

This has important implications for how a research endeavor is designed and executed, which is detailed in the rest of this section. The first subsection describes how the research focus was established, followed by a subsection arguing for the choice of a process perspective. The next subsection details the choice and design of a qualitative, single case study, concluding with a discussion of various considerations implicated in the choice of research design.

4.1.1. ESTABLISHING THE RESEARCH FOCUS

A central implication of the collaborative practice engagement form is the dedication to formulating research problems *with* (not for) practitioners (Nielsen and Persson 2016; Van de Ven 2007). Although each problem situation affords unique opportunities for addressing existing literature, developing theoretical frameworks, adopting various methods, and contributing to real-world problem-solving, deciding on all of these *before* engaging with the problematic situation is not possible (Mathiassen 2017). The methodological considerations going into the final choices of research design for this dissertation therefore build on experiences that were formed during preliminary engagements with practice. How this led to establishing the research focus is detailed below.

From the outset of the PhD study underpinning this dissertation, I was interested in understanding the organizing aspects of a growing data phenomenon. This interest developed during the final years of my graduate studies in IT, where the big data hype was at its peak, but few Danish companies had managed to realize any of its potential in 2016. Participating in a project with a large organization looking to develop an open data service confronted me with inherent tensions, contradictions and deep organizational difficulties; issues that were paid little or no attention in management literature often preoccupied with touting unlimited possibilities with new data-centric technologies. In passing, data governance was mentioned as a prerequisite for organizing data, but corresponding research proved scarce, underdeveloped and lacked empirical grounding (elaborated in Chapter 2).

The early perception of the research interest in data governance informed the choice to assume a preliminary empirical study. In engaged scholarship, the research process is

understood in terms of four different study activities (see Figure 3). Problem formulation seeks to ground and diagnose a problem up close with those who experience it in practice; theory building seeks to elaborate and justify a theory by engaging relevant disciplines; research design seeks to develop a model for studying the theory and; problem solving seeks to communicate and negotiate findings with intended audiences. While these activities may be performed and iterated in any sequence, Van de Ven notes:

> "[research methodology texts] tend to focus on research design and pay relatively little attention to the processes of problem formulation (…) while these texts provide good technical treatment of research designs and data analysis, they largely ignore social processes of engaging stakeholders in problem formulation" (Van de Ven 2007, p. 12)

Looking to not only ground the research, but also to develop a deeper appreciation for why governing data was difficult in practice, the preliminary study expressly adopted an engaged problem formulation approach (Nielsen and Persson 2016). Engaged problem formulation seeks to establish joint learning settings for practitioners and researchers, uncover and assess the assumptions of both practice and research underlying a problem situation, negotiate relevance and priority of problems and reformulate problems repeatedly in a given research process. This is embodied in three principles; problem dialogue, problem deliberation and problem flexibility. (Nielsen and Persson 2016, p. 733).

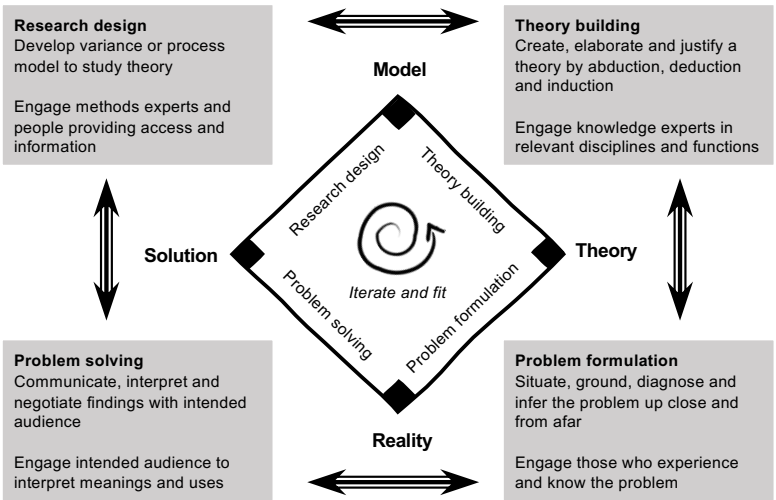

Figure 3 Study activities involved in engaged scholarship (reproduced from Van de Ven, 2007)

Only after defining the research interest and deciding the engaged problem formulation approach, the research setting was determined (elaborated in section 4.2). In early spring

2017, I was part of the DISIMIT network[5], which had hosted a series of workshops and conferences, under the common theme of exploring new data-centric technologies in local government. The events had high attendance rates and practitioners from various Danish municipalities were both enthusiastic about new opportunities and attentive to the challenges associated with the pending EU data protection regulation set to enter into force in May 2018 (see section 4.2.X). Engaged scholarship hinges on the willingness of practitioners to collaborate and co-produce knowledge with researchers. Thus, the enthusiasm and commitment demonstrated by municipal practitioners combined with their previous experiences with research-practitioner collaborations, were deciding factors in choosing Danish municipalities as a research setting.

Based on the principles of engaged problem formulation (Nielsen and Persson 2016), the preliminary study proceeded in the form of three formal workshops and four group interviews with a total of 34 representatives from 13 different municipalities (see Figure 4). The representatives were primarily IT and digitalization directors, but also counted internal consultants, project managers, developers and IT architects. The research activities sought to involve all three principles in order to collaboratively develop a deeper, mutual understanding of issues with data governance at the intersection of practice and research. Further details on methodology, empirical analysis and research contributions are reported as standalone results elsewhere (Benfeldt 2018; Benfeldt et al. 2020; Nielsen et al. 2018).

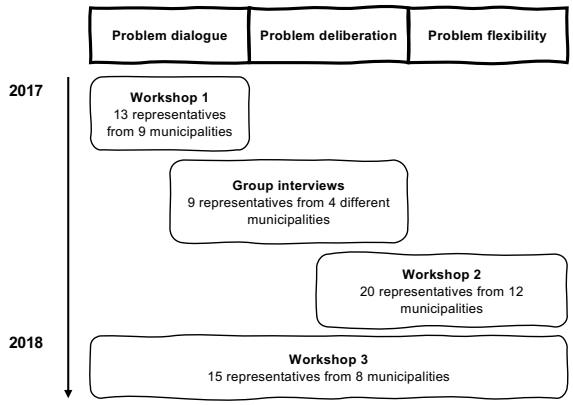

Figure 4. Research activities in the engaged problem formulation study

[5] DISIMIT is a joint research network, where researchers and practitioners from IT, digitalization or other functions in Danish local government engage in knowledge sharing and discuss common interests. The network started as a research project that ran from January 2009 to July 2012 with IS researchers from Aalborg University and 11 Danish local government municipalities (Rose et al. 2012).

The preliminary study had several implications for the final research focus in this dissertation. As anticipated by Mathiassen (2017, p. 18), when scholars become increasingly familiar with the problem situation and relevant theory, they need to adapt decisions and reconsider issues. My empirically grounded appreciation of the problem situation indicated the need for a novel theorization of key assumptions about data governance. Exploration of a collective action framing (Benfeldt et al. 2020) eventually inspired the theoretical framework guiding this dissertation (see Chapter 3), namely self-organized, polycentric governance (Ostrom 1990). The choice to pursue this theoretical framework in turn dictated subsequent decisions to conduct a qualitative case study with explicit process focus, explained later in this section 4.1.

A secondary outcome of the problem formulation process was the unexpected, meaningful partnerships I formed with practitioners from the participating municipalities. After a year of close collaboration, I had gained profound understanding of a complex, organizational context, while the practitioners had seriously embraced the idea and necessity of data governance. In the aftermath, Fairview municipality, which later became the empirical case for this dissertation, showed unforeseen initiative and invited me to host a full day workshop on data governance for their executive management group. This became a deciding factor in choosing to retain the municipality as a research setting, given that reliable access to information precedes other considerations in choosing the case(s) for a case study:

> "You need sufficient access to the potential data, whether to interview people, review documents or records, or make observations in the "field" Given such access to more than a single candidate case, you should choose the case(s) that will most likely illuminate your research questions." (Yin 2009, p. 26)

Further considerations on the municipality as a research setting are elaborated later (see section 4.2). Progression from initial formation of the research interest, to conduct of an engaged problem formulation study, to the choice of theoretical framing and research setting led to the establishment of the research focus for this dissertation. which was examining how a specific organizing logic evolved and enabled an organization to conceive data governance arrangements in response to emerging challenges and opportunities for data within and beyond their organizational boundaries.

As this subsection has covered the problem formulation activity, the diamond model of engaged scholarship (depicted in Figure 3) suggests a subsequent attention to theory building. This activity is covered later in section 4.3, and further expanded in Chapter 3. The following subsections will instead elaborate the research design, starting with the choice to pursue a process study.

4.1.1. A PROCESS STUDY

At the core of this dissertation is the dedication to studying how an organizing logic evolved over time. For research questions looking to understand how social issues emerge, develop and grow over time, Van de Ven proposes a process study:

> "'How' questions require a process model or 'event-driven' explanation of the temporal order and sequence in which a discrete set of events occur (…) Process studies are fundamental for gaining an appreciation of dynamic social life, and developing and testing theories of 'how' social entities adapt, change, and evolve over time" (Van de Ven 2007, p. 145)

Contrasted with variance studies, which instead are apt for addressing what-questions and considering outcomes or antecedents of an issue (Van de Ven 2007), certain assumptions underpin a process focus. These include attention to central subjects, like people, groups, organizations and material artefacts (as opposed to variables in variance studies), events as essentials units of a social process (as opposed to constructs), critical and conjunctive events as explanations of development and change, the importance of temporal sequence in events and emphasis on process narratives (Van de Ven 2007, pp. 155–157). These assumptions align well with the purpose of this dissertation, which seeks to understand and explain how a group of people within a municipality over time managed to devise organizational data governance arrangements.

Questions looking at change over time consequently call for longitudinal data that can be obtained either through retrospective accounts from historical archive files or from a real-time field study (Van de Ven 2007, p. 195). Opting for the latter allows researchers to observe the change process as it unfolds in the field setting and potentially discover any sudden, but important, transient developments affecting this change. Where variance studies emphasize a high number of cases selected for data collection, there is no obvious sampling scheme for process studies. Scholars may consider cases that offer extreme situations, polar types, high experience levels, or likelihood of access, and focus on any number of temporal events observed based on the duration and granularity of the change process in question (Van de Ven 2007, p. 212).

As disclosed earlier, this dissertation focused expressly on a single organization, Fairview municipality. Based on the interest and commitment in the early problem formulation stage, Fairview offered a high probability of future access to key subjects. Within more than a year, early observations from the collaboration with Fairview indicated a significant change in attitudes and behavior of key subjects (explained in Chapter 5) on the phenomenon in question. These observations informed the choice to focus on a single organization, but a higher number of temporal events (implications of this design choice are further discussed in section 4.1.4). For "few cases, many events" (Van de Ven 2007, p. 214), engaged scholarship proposes the qualitative case study design (Yin 2009), which is consistent with the choice in this dissertation and elaborated in the next subsection.

On a brief note, the theoretical framework further corroborated the decision to pursue a process study. Extensive case-study literature report on the characteristics of *on-going* self-organized, polycentric governance systems (see Chapter 3), but little is often known about the origins and early inception of such systems:

> "I examined [governance systems] that have survived for long periods of time in environments characterized by considerable uncertainty and change. (…) These cases demonstrate the feasibility of robust, self-governing institutions, (…) but the origins of these systems are lost in time. (…) We do not know who originated or opposed various proposals or anything about the process of change itself." (Ostrom 1990, p. 103)

A process study on how such an organizing logic emerges and evolves in an empirical setting over time therefore also offered an opportunity to develop a solid contribution to existing literature.

4.1.2. A QUALITATIVE, SINGLE-CASE DESIGN

Several points have been made until now about the choice to pursue a qualitative case study design. A case study is "an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" and is particularly appropriate, when addressing how or why research questions (Yin 2009, p. 18). These observations align well with the central research interest in this dissertation, which seeks to examine the process of how an organizing logic evolved and enabled key subjects within an organization to devise data governance arrangements in response to emergent challenges and opportunities from both within and beyond organizational boundaries. Such an inquiry is inevitably entangled with its context and concern a phenomenon unfolding in real-time (see section 4.1), making the case study design ideal.

The type of case study undertaken for the empirical inquiry explicitly involves a qualitative approach (see section 4.3 for empirical data collection methods and subsection 4.1.4 for implications of research design) and a single-case design (Flyvbjerg 2006; Stake 1995). In IS research, qualitative is often taken to be synonymous with interpretive (Walsham 1995), but not in the case reported on here. The qualitative approach in this dissertation empathizes with the interpretive approach to field studies on a number of issues, such as the importance of contextualizing a phenomenon in its historical, social setting, the rejection of "data as things" waiting to be gathered and the use of theories to view the world in different ways (Klein and Myers 1999), but the underlying philosophical assumptions resonate more with a paradigm of pragmatism (Elkjaer and Simpson 2015). Where interpretivism is concerned with understanding and pursuit of interesting knowledge, pragmatism is concerned with action and constructive knowledge (Goldkuhl 2012).

A qualitative case study with a pragmatist stance fits well with the overall engaged scholarship research approach. Engaged scholarship values co-production of knowledge *with* (not for) practitioners and attention to practical problem-solving in addition to rigorous theory development. Pragmatism explicitly seeks to create knowledge in the interest of change and improvement. These interests are not identical to the explicit interventions in the design and control types of engaged scholarship (see Figure 2 section 4.1) or action research (Baskerville and Myers 2004). Rather, it builds on the idea of empirical inquiry as a bounded investigation into some part of reality with the purpose of creating constructive knowledge for potentially enacting deliberate change in this part of reality (Goldkuhl 2012, p. 139). Though the inquiry itself may be local and contextual, there is a clear intention to produce scientific knowledge, both meaningful and useful, for practices beyond the ones studied (Goldkuhl 2008). Formulating how this knowledge applies beyond local practices is an explicit goal in pragmatist research. It is also reflected in the nature of this dissertation's research question, which seeks to explain how specific actions contributed to evolvement of a phenomenon in practice. In brief, the role of knowledge in pragmatism is to be useful for action and change, where the role of knowledge in interpretivism is to be interesting in itself (Goldkuhl 2012; Walsham 1995).

Opting for the single-case design (Flyvbjerg 2006; Stake 1995) consequently fits well with both the process perspective and the qualitative, pragmatist approach for several reasons. A single case offers the opportunity to gain in-depth, longitudinal insights about a bounded, complex phenomenon, which can be studied in its social context over time. Multiple formal rationales for choosing the single-case design exist. In a sampling logic, single-case designs are apt for the critical case, the unique case, the representative case, the revelatory case or the longitudinal case (Yin 2009). Strategic selection of cases can be based on extreme cases, maximum variation cases, critical cases and paradigmatic cases (Flyvbjerg 2006). In process studies (see previous section), scholars can go for extreme situations, polar types, high experience levels, or likelihood of access (Pettigrew in Van de Ven 2007, p. 212). Drawing on abovementioned (albeit not exhaustive) list, the rationales for choosing the single-case design includes a longitudinal outlook, with some revelatory potential and a high likelihood of access. Potential pitfalls and biases are discussed in detail in section 4.1.4 implications of design.

It should be noted that the nature of the case, especially in a single-case design, is likely to change as issues are investigated. The case may even turn out to represent a different sampling logic than initially determined (Yin 2009). For that reason, the choice of any case in single case designs likely involves a great deal of intuition, which must then later be accounted for and formalized:

> "We may select cases on the basis of taken-for-granted, intuitive procedures, but are often called on to account for that selection. That account must be sensible to other members of the scholarly communities of which we are part (…). All that researchers can do is use their experience and intuition to assess whether they believe a given case is interesting (…) and whether they can

> provide collectively acceptable reasons for the choice of case." (Flyvbjerg 2006, p. 233)

For exactly this reason, much criticism has been leveraged against the single-case design. Even if not made explicit, such critiques often work from positivist assumptions about social science research grounded in a natural sciences tradition (Klein and Myers 1999). Criticisms range from fears about "uniqueness" of the single case, vulnerability in putting "all eggs in one basket", skepticism about a researchers' ability to do empirical work beyond this one case (Yin 2009) as well as lack of generalizability and thus relevance, and confirmation bias (Flyvbjerg 2006). Although, for example, interpretive, single-case studies can offer analytical or theoretical generalizations in terms of concepts, theory, specific implications and rich insights (Walsham 1995), it is unlikely that cases of any number will be a strong representation of others for a simple reason:

> "Case study research is not sampling research. We do not study a case primarily to understand other cases. Our first obligation is to understand this one case (…) How shall cases be selected? The first criterion should be to maximize what we can learn." (Stake 1995, p. 4)

Multiple reasons supporting the rationale for a qualitative, single-case design can be summarized now. In this dissertation, a single case allows for in-depth insights about a phenomenon as it develops over time, which underpin the choice to pursue a "few cases, many events" type of process study. Secondly, a foundational pillar of engaged scholarship is the establishment of joint learning settings to facilitate co-production of knowledge with practitioners, which takes time. Concentrating research efforts in an already-established setting thus ensures that (limited) resources are spent on obtaining insights about the phenomenon under study, rather than on establishing rapport or gaining access to new sites. Arguably, a longitudinal case with reliable access to information increases the potential to learn about the research interest.

Significant intellectual costs are associated with getting acquainted with a new social context. While multiple cases may increase statistical generalizability or satisfy positivist sampling logic, it does not resonate with a qualitative, pragmatist approach. Here, the objective is careful, deliberate formulation of instrumental knowledge, how it applies beyond the locally studied practices (Goldkuhl 2012) and not the achievement of statistically generalizable results based on a representative number of cases. Besides:

> "from both an understanding-oriented and an action-oriented perspective, it is often more important to clarify the deeper causes behind a given problem and its consequences than to describe the symptoms of the problem and how frequently they occur." (Flyvbjerg 2006, p. 229)

Further reasoning about choosing Fairview municipality as a case and why it offers a high potential for learning about the research interest are unfolded in section 4.2. Before that,

the next subsection will conclude the research design section with a discussion of key implications.

4.1.3. IMPLICATIONS OF THE RESEARCH DESIGN

So far, this section has dealt with the motivations for pursuing a collaborative practice form of engaged scholarship, including how establishing the core research focus led to the conception of a process study with a qualitative, single-case design. Inevitably, this research design has had several implications for the way the empirical inquiry is conducted and evaluated. Studying a sociotechnical phenomenon over time, in its real-life context requires access to and insights about people, groups and artefacts, which also has implications for the choice of research setting and the gathering of empirical material. Any such implications are examined in section 4.2 and 4.3 respectively. The remainder of this section will focus on the role of the researcher in conducting a qualitative case study from a pragmatist stance and the quality criteria for evaluating results from a theory development-oriented single-case design.

4.1.3.1 The role of the researcher in qualitative, pragmatist-oriented research

In engaged scholarship, the role of the researcher is at the forefront; explicit and present. Albeit in collaboration with experts, stakeholders, practitioners or other researchers, an engaged scholar actively situates and grounds problems, creates and justifies theory, develops and assesses models, communicates and negotiates findings (Van de Ven 2007, pp. 10–11); an engaged scholar makes judgments about relevant literature, problematizes assumptions, makes preliminary assessments and even constructs opportunities for making contributions (Mathiassen 2017, p. 19). For the collaborative practice form specifically, it is advised that a research team is composed of people with previous experiences and demonstrate "an intrinsic motivation in the problem being investigated" (Van de Ven 2007, p. 277).

Such active involvement stands in stark contrast to some traditional ideals of the researcher in qualitative case studies. In positivist-oriented case studies, the researcher must not be "trapped" by their own ideologies; they must, from the beginning, have a firm grasp on the issues being studied, but they must also be unbiased by preconceived notions, even those supported by theory (Yin 2009, p. 69). In interpretive case studies, researchers must be critical when they socially construct research material with participants; but also recognize how their inquiry alters participants' understanding of their own world and analyze how informal contact, conversations or specific requests for material shape how individual subjects consequently represent their affairs to the researcher (Klein and Myers 1999, pp. 81–82). Yet, for pragmatist-oriented case studies, an involved researcher is quintessential:

> "Pragmatism emphasizes the active role of the researcher in creating data and theories. Experimentation in the world is pivotal. The researcher is participating in practice in order to explore – through personal actions or close observations of others' actions – the effects and success of different tactics." (Goldkuhl 2012, p. 141)

The role of the researcher from a pragmatist stance is therefore not to seek impersonal, unbiased accounts or access and acknowledge subjective interpretations of the case. Rather it is to actively participate in the setting(s), where knowledge about the phenomenon of interest can be co-produced with - or in close observation of - others.

Expectations for experimentation and participation in this sense should not be confused with that of other interventionist approaches, like action research (Avison et al. 1999; Baskerville and Myers 2004), design science (Hevner et al. 2004) or action design research (Sein et al. 2011). Pragmatist-oriented research is concerned with constructive knowledge that can inform deliberate attempts to affect change beyond the studied context. A key distinction remains: where formal interventionist approaches must enact local change and may contribute to general practice, pragmatist inquiry may enact local change, but must contribute to general practice (Goldkuhl 2008). A researcher in this type of inquiry is therefore not only concerned with knowledge for explaining (primary interest in the positivist tradition) and understanding (primary interest in the interpretivist tradition), but also for prospecting; for entertaining ideas about what might be in a future, not-yet realized social world (Goldkuhl 2012)

Participation of this kind warrants reflexivity on part of the researcher. Reflexive research practice involves continuously questioning taken-for-granted assumptions about the nature of social reality, knowledge, and the validity of methods of inquiry, both in relation to the organizational setting(s) under scrutiny, but also within researchers themselves (Cunliffe 2002, 2003). Reflecting on and confronting the self-other relationship is to some degree a built-in feature of engaged scholarship, since a core research activity seeks to uncover and assess assumptions underlying a problem situation from both practice and research perspectives (Nielsen and Persson 2016; Van de Ven 2007). Self-reflexivity calls for the individual researcher to direct attention to how their own disposition(s) can shape the way they capture interactional, complex social experiences and that such dispositions be made known, for example through confessionals, textual strategies or stories about fieldwork experiences (Cunliffe 2011).

Throughout the course of the PhD study underpinning this dissertation, I have remained reflexive about my role as a researcher. My multidisciplinary affiliations[6] have allowed me to present, discuss and review my academic work with scholars from vastly different research traditions, in turn pressure testing vaguely defined concepts, taken-for-granted ideas about research methodology, unsupported knowledge claims and weak argumentation. Multiple practice collaborations with IT practitioners and managers, both attached and detached, have familiarized me with how to observe, capture, negotiate and participate in complex sociotechnical practices in real-life settings. My experiences may on one side represent a blind spot, in the sense that I have grown accustomed to unconsciously "backgrounding" issues of controversy, in favor of adhering to dominant group norms. Yet, I am also attuned to how multiple worldviews overlap and co-exist in organizational settings and I have become well-versed in how to appreciate and constructively manage their divergence and potential for conflict.

I have also been confronted with my assumptions as a researcher in a more explicit manner. While attending a PhD course specifically on approaches to reflexivity in organizational research, it was pointed out to me that I conveyed my empirical material in a manner often associated with positivist knowledge traditions (Cunliffe 2011). This was an unexpected, but a welcome revelation. I had previously examined and argued for explicitly rejecting a positivist approach to my research interest (Benfeldt 2018), yet my vocabulary and style seemingly gave the opposite idea. Although section 4.4 argues for the choice to conceptualize and present my empirical material through "realist tales" (Van Maanen 2011), I should like to acknowledge explicitly that any such connotations of realism resonate with what Goldkuhl (2012) tentatively terms the ontology of pragmatism; "symbolic realism", with heavy emphasis on the symbolic. While qualitative pragmatist research accepts that things or events studied within an inquiry can exist independently of observers, the approach maintains that any such elements originate in social meanings, reason and thought; not in a true, objectively existing reality (Goldkuhl 2012, p. 142).

Researchers must remain reflexive about their own role and engagement on two dimensions; careful interpretation of multiple or divergent meanings in empirical material and reflection about the researcher's own role, personal viewpoints and assumptions (Van de Ven 2007, p. 291). Although inward reflection is a necessary precursor, engaged scholarship emphasizes specifically the need to perform a "reality check" by engaging others in discussion about the researcher's assumptions. Such reality checks were sought

[6] As a researcher, I have been part of research groups at departments of Political Science, Computer Science and Computer Information Systems; as an engaged scholar, I have been part of a large practitioner-researcher network and managed my own research project with multiple practitioners in a single organization; as a PhD student, I have been enrolled in a Doctoral School of Social Sciences, but shared office space with PhD colleagues from the Technical Doctoral School of IT and Design.

by attending methodology courses; continuously sharing observations from the field with practitioners to gauge their response; discussing experiences from the field with fellow researchers continuously throughout the study and presenting papers at academic conferences to engage discussion.

4.1.3.2 Quality criteria for a theorizing-oriented case study

Formal conventions for evaluating qualitative case studies in IS research have been established and widely accepted for both positivist (Benbasat et al. 1987; Yin 2009) and interpretivist approaches (Klein and Myers 1999; Walsham 1995, 2006), but no corresponding, formal criteria exist for evaluating case studies from a pragmatist philosophical perspective. A lack of formal principles for evaluating the quality of a research design, consistent with its underlying philosophical assumptions, increases the risk that case study results will be misjudged or deemed inadequate (Klein and Myers 1999, p. 68). As noted earlier (in section 4.1.3), such is often the case for many of the criticisms levied against the single-case design, which can be said to feature positivist assumptions in disguise. To enable the reader to follow how results derive from initial questions to final conclusions, the remainder of this subsection will argue for evaluating the validity of this study through a criterion of "usefulness" (Goldkuhl 2012; Weick 1989) and demonstrate how it has been addressed throughout the dissertation.

First, being clear about how design choices tie in with foundational research objectives can help alleviate weaknesses in a single-case design (Benbasat et al. 1987, p. 383). Overall, the purpose of this dissertation is to develop novel theoretical ideas about a contemporary sociotechnical phenomenon (data governance as a set of digital practice involved in the organizing of data) for an IS research field in which such theorization is currently lacking (see Chapter 2). Yet, theory development in this study is not primarily concerned with knowledge for explanation (as in positivist traditions) or understanding (as in interpretivist traditions), but knowledge, which is useful for action (as in pragmatist traditions). In this sense, developing useful knowledge is not only about contributing to resolution of real-life problem-situations in organizational data governance. It is also about contributing new concepts that are useful for researchers in coping with, reasoning about and further investigating the many, multifaceted issues implicated in the sociotechnical data phenomenon.

Contributions of the latter kind echo recent calls for IS research to expand theory development beyond the traditional, formulaic studies that test obvious or common-sense relationships (Hassan and Lowry 2015). Most IS research tends to adopt a "mid-range script", where reference theories from other disciplines are instantiated, validated and tested, but very little is done to add new constructs, modify concepts or extend the theory to IS contexts (Grover and Lyytinen 2015). Although the script satisfies prevalent views on what constitutes legitimate IS knowledge, it produces a wealth of incommensurate, mid-range models which impedes the novelty and foresight needed to achieve scientific breakthroughs (Grover and Lyytinen 2015, p. 286). In addition,

research designs that are undergirded by methodologies in favor of validation, rather than usefulness tend to produce "trivial theory" (Weick 1989, p. 516) and empirical inquiries content with "repeating facts" (Goldkuhl 2012, p. 140) are unlikely to produce the evidence necessary for addressing enduring questions in the IS field (Grover and Lyytinen 2015, p. 285).

For overcoming inertia in theory development and cultivating more innovative IS theory, Grover and Lyytinen (2015) encourage "blue ocean theorizing" as:

> "unfettered theorizing about IT and related phenomena [that] allow greater liberties to build and abstract independent accounts of observed behaviors – accounts that are free from the need to justify them by recourse to reference theory or from the need to immediately validate them through testing." (Grover and Lyytinen 2015, p. 287)

Budding theoretical guesses or "sketches" may be difficult to evaluate and they may even be wrong, but their advantage in stimulating further discourse will exceed the potential costs of being wrong. By encouraging researchers to actively entertain ideas about "what could be", blue ocean theorizing in effect expands the epistemic script in IS to also include constructive knowledge which in itself is meant to inform and stipulate further discussion and inquiry (Grover and Lyytinen 2015, p. 287). This constitutes a starting point for considering useful as a criteria in research design, since the quality of these (blue ocean) contributions does not depend on whether the knowledge is generalizable or empirically validated, but rather "in the suggestion of relationships and connections that had previously not been suspected; relationships that change actions and perspectives" (Weick 1989, p. 524).

A quality criterion for useful knowledge does not mean "anything goes", but that any derived theoretical propositions are valued for their *plausibility* rather than for how accurately they claim to represent an objective reality (Weick 1989). For a theoretical idea to be plausible, it needs to be more comprehensible, incorporate more of observed data and remain more resilient in the face of criticism than a rival idea, and it is more likely to be perceived as such, if it taps into issues of the current climate, is consistent with other data, facilitates ongoing projects, reduces equivocality and offers an "aura of accuracy" (Weick et al. 2005, p. 415). The point is that if all theories are false (Mintzberg 2005, p. 355), but plausible theories are enough to enable action-taking, which then generates new opportunities for observing and incorporating data, which builds resilience and makes the theory more comprehensible, then plausible theories can be considered useful knowledge (Weick et al. 2005).

In this dissertation, plausibility is embedded in the premise of engaged scholarship, where involving multiple perspectives from a variety of relevant stakeholders constitutes a form of triangulation on the given research problem (Van de Ven 2007, p. 284). Engagement as triangulation is not about a technological solution to data collection or converging on one true explanation of an issue (triangulation as reliability), but about bringing forth as

many different, divergent perspectives as possible to observe inconsistencies, address criticism and reconcile fragmentations, which in turn increases the plausibility or "potency" of a given explanation (triangulation as validity) (Mathison in Van de Ven 2007, p. 286). Plausibility has been addressed through engagement with practice and seeking deliberate feedback from multiple academic environments during the empirical inquiry and the theoretical development.

On a final note, what separates a qualitative, pragmatist-oriented case study from more traditional approaches is not how it is designed or conducted, but rather how results are viewed. Since the processes of crating theory are different from those of testing theory (Mintzberg 2005, p. 358), it makes little sense to consider the quality of a blue ocean theory development-case study in the same manner that formalized tests and principles are used to check reliability and systematicity in mid-range case studies, of both positivist and interpretivist character.

This does not mean researchers are exempt from cogently explaining and motivating ideas, constructs or research design choices (Grover and Lyytinen 2015; Weick 1989). Careful attention has been paid in elaborating any underlying philosophical assumptions or methodological considerations that went into conceiving the research design for this dissertation. Formal data collection methods and case study tactics such as engaging multiple sources of evidence, keeping a database and using a case study protocol, (Yin 2009) have also been applied and are detailed in section 4.3. Further considerations on how empirical material and analysis informed theory development are elaborated later in section 4.4, while the next section will proceed with a description of the research setting, and details about the chosen case organization, Fairview municipality.

4.2. RESEARCH SETTING

As mentioned, the empirical inquiry in this dissertation involves a single-case study of how an organizing logic evolves and enables specific actions within Fairview municipality over a period of time. While contextualizing an overall research endeavor can help enrichen appreciation of subsequent empirical analysis and theory development, knowing the research setting and understanding how it was established also has important methodological implications for this study. As the collaborative form of engaged scholarship rely on co-production of knowledge with stakeholders in joint learning settings, rather than data collection sites, this section will begin by recounting how such a setting was established and how it led to Fairview as the chosen case organization. This is followed by a brief consideration of the surrounding context, since significant moves within national and international arenas intertwined with events unfolding within Fairview before and throughout the study. The section concludes with a description of Fairview municipality as an organization.

4.2.1. ESTABLISHING THE RESEARCH SETTING

As noted earlier, the foundation for the research endeavor in this dissertation was established as part of prior engagements with practice. After systematically reviewing available data governance literature (Nielsen 2017) and finding a consistent lack of empirical studies, I decided to pursue an empirical inquiry to understand how formal data governance approaches resonated with practice. Van de Ven (2007, p. 275) suggests that junior scholars should not "go at it alone", but rather take advantage of the relational network of senior colleagues in contacting and accessing practitioners for a study. Choosing Danish municipalities as the setting was therefore shaped by my membership of DISIMIT, which originated as a collaborative research project looking to improve the use of IT in Danish municipalities (Rose et al. 2012) and continued as a research-practitioner network.

I had participated in multiple events hosted by the network, which centered on the theme of data-centric opportunities in local government, and my relationships with senior scholars in the network facilitated relationship-building with other practitioners, who in turn were used to engaging with researchers on both practical and academic topics. While the workshops detailed in section 4.1.1 formed the basis for a separate problem formulation study, they were also essential in establishing the research setting going forward. Contributions from 13 different municipalities helped me get acquainted with heterogenous aspects of the problem of organizing data, such as municipal size, geographical placement, demography, history, political orientation and such, but also the enduring commonalities across municipalities, such as decentralized IT acquisition, the many professional domains and ambitious national strategies for digitalization. At the conclusion of these workshops, I gained a sincere appreciation for the organizational difficulties facing municipal IT practitioners in relation to data governance (Nielsen et al. 2018) and formulated a much clearer research interest (Benfeldt 2018).

After the engaged problem formulation, the IT director and Digitalization director from Fairview municipality, who had participated in all the workshops and offered to participate in the individual interviews as well, invited me to present the results to their executive management group. The enthusiasm and commitment demonstrated by these practitioners informed my decision to pursue a single case study with Fairview. Not only had I developed good relationships, but I also acquired a basic understanding of the organizational setting, which made it easier for me to identify key subjects. As noted in section 4.1, access to empirical material precedes other concerns in finding candidates for a case study (Walsham 1995; Yin 2009), while choosing case(s) that are hospitable to the inquiry maximizes potential for learning about the research interest (Flyvbjerg 2006; Stake 1995).

For collaborative practice research, prospective solutions are secondary to the importance of research questions, since good questions are more likely to motivate the attention and enthusiasm of practitioners (Van de Ven 2007, p. 275). Likewise, a

collaborative relationship is premised on common desire to learn about a problem. Looking to sustain the engagement of Fairview municipality and align roles and expectations in the coming project, I consulted with the digitalization director about what kinds of problems or issues we could converge on as being of mutual interest. Since Fairview had worked hard to implement data governance arrangements for ensuring GDPR compliance, we agreed that following this process, reviewing its progress and identifying any secondary benefits for the municipality would constitute the collaborative research project. Further details on this process are detailed later in section 4.2.

On a final note, spending time within the research setting is critical for building relationships, trust and learning among researchers and practitioners (Van de Ven 2007, p. 292). Longitudinal studies promote more profound insights of a subject matter, not only because repeated participant interactions over time lead to greater candor in responses, but also because familiarity with the setting enables the researcher to ask more probing questions and engage more deeply with issues. It takes significant amounts of direct and personal investigation to become acquainted with the dimensions and context of a phenomenon. In light of the time and effort required to establish genuine relations with practitioners, I decided to pursue a single rather than comparative case study. While two cases would offer some cross-case reliability and likely dispel potential criticisms of uniqueness or confirmation bias, the energy spent on building relationships in a similar way would waste precious resources and dilute existing participation in the research setting in Fairview.

4.2.2. THE CONTEXT OF DANISH MUNICIPALITIES

A basic premise of case studies is that boundaries between the phenomenon and the context are not clearly evident (Yin 2009). Accounting for context is essential, since it may have both subtle and powerful effects on organizational behavior (Johns 2006). Studying how field-level dynamics intersect and co-evolve with organizational processes can be understood through processes of zooming-in and zooming-out on practices as they unfold (Nielsen et al. 2014), rather than considering a cause-effect relationship between contextual factors and organizational behavior. The following subsection briefly accounts for significant developments in surrounding arenas, which directly and indirectly emerge as part of the case study involving Fairview municipality.

Denmark is a consensual and technologically advanced society. Digitalization has been driven through comprehensive national strategies for increasing efficiency of the Danish public sector through use of IT in state, regional and local government. A tradition of high ambitions for digital administration has led to the establishment of central CPR (citizens) and BBR (building and housing) registers (Rose et al. 2012) as well as common digital mail (e-boks), common digital ID signature (NemID) and a one-stop portal for citizens to engage with government services (borger.dk). The newest digital strategy for 2016-2020 is no less ambitious than the previous ones. Yet, the emphasis has shifted to focus heavily on ambitions for data use in the Danish public sector. Numerous goals

specifically aim to incorporate data to enable better and quicker case processing, to exploit data assets as a driver for economic growth, and to protect citizens' individual data privacy rights, while underscoring the role of local government in realizing these initiatives (Agency for Digitisation 2016).

While interpreting the national digital strategy entails complexities of prioritization, it is highly influential on local government practice (Persson et al. 2017). Danish government is somewhat decentralized, which means that Danish municipalities are not merely executing central government orders but have a great deal of autonomy in how their managers and elected officials choose to organize the delivery of public services. Although public administration in Denmark has been at the frontiers of digitalization since the 1960s (Rose et al. 2012), IT acquisition has historically been decentralized. Focused on highly specialized solutions to fit individual domain need, a wealth of systems have accumulated within a municipality over time and current IT architecture consists of "spaghetti integrations", which were expensive to develop and even more expensive to maintain (Digitaliseringsstyrelsen 2018). As a result, a single municipal organization is tasked with storing, collecting, and administering vast amounts of heterogeneous, and at times redundant, data across its many different systems.

With the instatement of the European General Data Protection Regulation (GDPR) (European Union 2016), managing municipal data is not only about achieving strategic objectives, but about devising governance arrangements to ensure legal processing. The directive entered into force from May 25, 2018, and fundamentally reshaped how personal, private and sensitive data are handled any organization in order to protect individual rights to data privacy (European Commission 2018). Personal data[7] may only be collected and processed if under one of six lawful bases and data collected under one purview may not be reused in other contexts not covered by the same purview (European Union 2016). As data processors, municipalities must be able to at all times demonstrate, they have implemented the necessary technical and organizational governance mechanisms to ensure compliance with the regulation. As a consequence of numerous digitalization efforts over the years, Danish municipalities collect and store massive amounts of personally sensitive data on citizens, both inadvertently and purposely, just to perform their duties. Yet, no standards or collective approach were devised for exchanging data effectively or safely across national, regional or local boundaries; legal permissions for data collection and sharing were either decided ad hoc or not at all, and; since thousands of public IT systems were not made to speak a "common language",

[7] Personal data is data relating to a living individual who can be identified from those data alone or from those data in combination with other data, that are *likely* to also exist in the same context and may only be processed: with consent from the individual, as necessary by a contract with the individual, as part of a legal obligation specified by law, to perform interests vital for the individual, as part of a public function or task sanctioned by regulation, and as part of a legitimate interest within the organization

complexities multiply because the same data has to be collected multiple times (Digitaliseringsstyrelsen 2018).

For a single Danish municipality, efforts to devise appropriate governance arrangements are therefore complex because they are heavily entangled with dynamic processes beyond their own organizational boundaries. Individual municipalities may now have great autonomy in how they choose to maintain and develop IT and digitalization initiatives, but all solutions in the public sector were previously developed and maintained by a single developer, KMD. Until 2009, KMD was owned by the municipalities themselves through the interest organization Local Government Denmark, which promotes continuous development, support and innovation in local government. To facilitate the transition from monopoly, a new non-profit organization, KOMBIT, also owned by the municipalities, were established to assist the 98 municipalities in migrating from the many proprietary, professional systems (KOMBIT 2018). A more open market for soliciting public sector IT solutions promotes fair competition and obliges municipalities to send all major IT projects into official tender, but since many proprietary systems developed by KMD still remain in use, restricted access to data and limited options for integration do little to reduce complexity.

In an attempt to curb these challenges, KOMBIT has devised a common digital architecture framework to foster integration across municipal solutions. The purpose was to share infrastructure modules, promote open standards, ensure component reuse and reduce reliance on proprietary solutions (Digitaliseringsstyrelsen 2017). The framework elaborates understanding of and processes for developing best practice IT architecture in a municipality, but it is up to the individual municipalities to ensure these are implemented in their IT development projects. Based on the architecture framework, KOMBIT has also developed a common municipal infrastructure, which includes specific requirements for ensuring data integration and certain joint municipal IT solutions (KOMBIT 2020).

Recognizing that much can be gained from openly collaborating, five municipalities founded an open source development group amongst themselves in 2012 (OS2 - Offentligt digitaliseringsfællesskab 2014). The OS2-community seeks to develop standardized modules for public IT, which are based on open source technology and openly shared amongst members of the community and has since its inception expanded to include other municipalities and public organizations as well. Members pay an annual fee and as of 2020, the community consists of 71 public organizations (of which 67 are municipalities), 63 suppliers and 22 open source solutions, including systems for remotely managing access to government devices, a data crawler for identifying sensitive person data and an overview tool for managing all IT systems in a municipality.

While numerous interest groups and associations shape data governance arrangements in a municipality indirectly through architectural principles and open source IT solutions, additional authorities and committees directly influence how data can, must or should

not be treated. The Danish Data Protection Agency has existed since 1979, but became significantly more prominent in municipal settings when GDPR was set to enter into force in 2018. As an independent authority, the agency advises on regulations for processing personal data and supervises that authorities, companies and other data controllers comply with data protection rules. Their main tasks include performing regular audits of organizational data governance arrangements underpinning GDPR compliance; investigating data rights violation complaints; reporting violations to police and registering any data leaks reported by organizations. A year after GDPR entered into force, the agency experienced 150% increase in their main activities (Data Protection Agency 2019). In extension, an official data ethics committee was formed in early 2019 with member experts from business, IT, human rights, healthcare and communications research. The overall purpose of the council is to encourage public debate about data rights, promote sustainable, responsible development of data-centric technologies in both public and private sector organizations, and advise parliament, ministries and public authorities on how to implement data ethics (The Ministry of Justice 2019).

For a single municipality, devising data governance arrangements for responding to opportunities and challenges is not an isolated endeavor constricted within organizational boundaries, but co-occurring with other processes at multiple levels in surrounding arenas. Further details on how zoom-in and zoom-out perspectives informed the empirical analysis are elaborated in section 4.4.

4.2.3. THE CASE OF FAIRVIEW MUNICIPALITY

Fairview municipality is an above average size municipality located in Denmark amid large forests, hilly terrains, intricate lake systems and fertile soil. The population in Fairview counts +60,000 citizens but has increasingly come to function as a suburban area for more metropolitan cities in the surrounding municipalities. This is also reflected in the demographic composition (see Figure 5), with majorities in the preteen, middle-aged and older populations. Fairview is also a relatively wealthy municipality, where the average yearly income per person in 2016 ranged between DKK 300.000-325.000 (approx. EUR 40.000-43.000) (Cevea 2017), the second highest income group for Danish municipalities.

Like other Danish municipalities, Fairview municipality is responsible for delivery of numerous public services, colloquialized under the umbrella term "citizen-directed tasks" in their designated geographical area. These broadly include social services, like childcare, primary schooling, homecare, disability support, employment initiatives and social integration as well as environmental services, like infrastructure maintenance, water supply, waste disposal, urban planning and cultural offers. Fairview organizes the delivery of these many services with outset in a specific model, termed the Fairview model. The Fairview model emphasizes decentralization, local decision-making, short communication paths and clear political influence, and posits that responsibility should be delegated to those closest to where decisions are implemented. In Fairview, a number

of institutions, centers and organizations delivering specific public services are accountable directly to the city council, and not a manager of a specific department or professional secretariat. Referred to as 'contractors', their responsibilities and budgets are determined yearly in direct negotiation with members of the city council and include primary schools, daycare institutions, homecare facilities, libraries and recreational centers. While directors of these institutions work closely with administrative staff in Fairview's eight main departments, they are autonomous entities in themselves and decide how to manage budgets, employees and other administrative behavior.

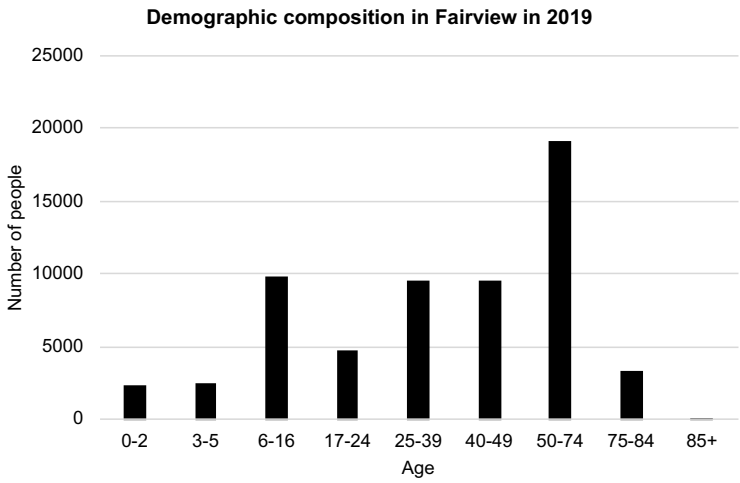

Figure 5. Demographic composition in Fairview municipality in 2019

Implicated in the Fairview model is also a division of labor, where the city council with its 29 elected officials set the overall direction by delegating financial funds, devising strategies and developing policies, which are then enacted by aforementioned contractors in addition to eight centrally placed administrative departments; four professional domain secretariats and four administrative departments. The role of these departments is to collaborate with and support individual contractors in enacting the decisions and policies defined by the city council and the municipal board of directors. The four professional secretariats handle domains which involve direct interactions with citizens and include Technical and Environmental Services; Employment and Health; Children and Youth as well as Elder and Disability. The four administrative departments handle mostly supporting functions and include the City Council and Executive Office; Human Resources; Finance, Innovation and IT as well as Culture, Citizen and Planning. Each department is led by a director, who is also part of Executive Group Management along with three members from the Board of Directors. In total, Fairview employs +5,000 people, from local contractors to individual directors on the board.

In Fairview municipality, the IT/Digitalization and Business Development team (from now on IT and Digitalization) is placed within the Finance, Innovation and IT department along with four other functions; Budget and Analysis; Finance; Purchasing and; Maps and GIS and directed by a CFO. In the beginning of the empirical inquiry, Fairview employed both an IT manager and a Digitalization director, but at the end, the Digitalization director had temporarily absorbed the responsibilities of the IT manager, since the person occupying the role had quit and the process of finding a replacement was still ongoing. In addition to technical support staff, the IT and Digitalization team counts an information security coordinator, and several IT developers, consultants and IT project managers.

Like at national level, digitalization efforts in Fairview are also driven by a digitalization and IT strategy, which sets a common direction for the entire organization, encompassing both the centrally placed administrative departments and secretariats, as well as the local contractors. For the strategy spanning 2017-2020, the main purposes of digitalization were to contribute to coherent user experiences for citizens, companies and employees; continued streamlining of daily operations; secure storage and processing of data and; better implementation of digital solutions and benefits realization. Particular emphasis was placed on the importance of IT architecture principles in acquisition and development of new solutions:

#	IT architecture principles
1	IT solutions must promote coherence, efficiency and innovation in the interaction between citizens, companies and Fairview Municipality
2	Use IT architecture that aligns with common strategy and technology choices and supports common platforms
3	Apply open, international standards, integration patterns and "Best Practices" with a view for how IT solutions must be able to communicate efficiently and cross-functionally
4	The entire product life cycle must be considered
5	All IT systems must be documented in Kitos[8]
6	Digitization and Business Development must always be conferred when purchasing new solutions

Table 7. IT architecture principles for Fairview municipality

The autonomy of individual departments warranted by the Fairview model means that IT acquisition and development across the municipality are not centrally coordinated by,

[8] A dedicated overview tool for managing all sorts of different IT systems in a municipality

but subsequent management and support of any purchased solutions are delegated to the IT and Digitalization department. To maintain an overview of the IT systems, ensure integration between new and old systems and check requirements for data sharing and security, the principles encourage individual contractors and departments engage with the Digitalization team so that new solutions remain both appropriate for the professional domain but also compatible with other systems and sustainable in the long run.

4.3. EMPIRICAL MATERIAL

Having decided on a qualitative case study with longitudinal does not automatically determine methods and strategies for how to gather empirical material on the phenomenon under study. Longitudinal process studies of organizational behavior and change often involve different forms of data collection such as archival, retrospective and real-time observations (Van de Ven 2007). While real-time observations offer the opportunity to observe short-lived events with great impact, it is not always possible to know whether or when this will occur. Retrospective accounts and archival material can produce fruitful insights "after the fact", since given outcomes are known and can thus be studied retrospectively.

For this dissertation, a fundamental distinction is made between data sources and methods for generating data from these sources (Mason 2002). This distinction goes beyond letting the choice of methods dictate the type of data which can be collected and instead focuses on what insights are needed to say something about the phenomenon in question. The rationale for linking the two derives from the research question, that is "what am I interested in knowing something about, what (or who) might be able to offer this insight and how will I be able to obtain this insight" (Mason 2002). Adopting this approach not only prompts the researcher to ensure the philosophical assumptions underpinning design correspond to how insights are generated, but it also offers transparency and enables the reader to judge the validity and reliability of final results on the basis of methodological choices (Yin 2009).

4.3.1. GENERATING EMPIRICAL MATERIAL FROM DATA SOURCES

For the empirical inquiry in this dissertation, deciding on data sources and methods involved asking the central question: how does one study an organizing logic? From the working definition (see Chapter 2), an organizing logic relates to managerial rationales for evolving specific arrangements. This would point to plans for data collection centered primarily on interviews with various individuals in Fairview, looking to generate insights about any underlying motivations and explanations for how and why certain data governance arrangements in Fairview were evolved or designed in the ways they were. Yet, early engagements with Fairview and similar organizational settings from the problem formulation study (See Figure 4 and Nielsen et al. 2018 for further details)

revealed that focusing primarily on interviewing as a method would not offer the types of insights I was interested in.

The interviews were dependent on my ability as an interviewer to know exactly what knowledge to inquire about, but the paucity of theory and operationalized constructs offered by the data governance literature produced inadequate, narrow interview guides which then also became constrictive in my further collaboration with practitioners. The normative assumptions embedded in the frameworks, and thus conveyed in my subsequent interview guides, made practitioners feel inadequate and as one project manager remarked, when I inquired about who it would make sense to talk to in a municipality about data governance:

> "You are probably on the bleeding edge there and a little ahead of the actual insights out in the business, even private companies, so there would be someone who can see this well, but the vast majority of professional managers and employees, they would be somewhat unsure of where they are" (Project manager, Group interviews, June 2017)

Relying on interviews worked well for gaining broad understandings and reflections, but also proved too snapshot-like (Mason 2002a) for providing deeper processual insights about how the organizing logic evolved over time, since it hinged on subjects' ability to recall and reflect on actions they had taken in an artificial setting (Patton 2002). Thus, interviews were combined with observations and internal documents to produce knowledge about actions in a process perspective. These methods aligned well with the pragmatist approach to qualitative research, which let actions, practices and activities become the primary vessels for studying a phenomenon (Goldkuhl 2012), more so than subjects' beliefs or individual interpretations of the phenomenon. Observations of practice in Fairview allowed me to study how specific actions were taken in devising data governance arrangements and how these actions over time from a theoretical perspective enacted an organizing logic. The methods combined to produce the type of knowledge I am interested in and believe to be possible to obtain in this inquiry.

On a final note, referring to data collection as "Generating empirical material" is a deliberate choice to signal that I have not been a passive gatherer of facts nor is the use different methods an attempt to obtain more accurate truth (Mason 2002). As previously noted, triangulation (as validity) is embedded in engaged scholarship, where the involvement of multiple stakeholders *intentionally* seeks to bring forth multiple, often divergent perspectives on a problem situation because it produces more penetrating insights and increases the "potency" of a given explanation (Van de Ven 2007). Consolidating such material by observing inconsistencies, addressing differences and reconciling fragmentations is expected of and by the engaged scholar. My movements, questions and presence in the setting have not been about excavating knowledge, but rather (re)constructing knowledge with practitioners (Mason 2002).

4.3.1.1 Interviews

Interviews are an established method in qualitative enquiry with a longstanding tradition in IS research (Myers and Newman 2007; Myers and Walsham 1998), and may range from the structured standardized interview, the semi-structured interview to the informal conversation (Patton 2002). Qualitative interviews are apt for inquiries, where social explanations and arguments build on depth, nuance, roundedness and complexity in data, rather than broad patterns or surface explanations (Mason 2002b).

The empirical inquiry in this dissertation adopted a mix of informal conversations, semi-structured individual interviews and semi-structured group interviews, listed in Table 8. Individual interviews focused on types of questions (Patton 2002) related to; experience and behavior to understand both past and present actions, since these are of primary concern in a pragmatist-oriented case study (see section 4.1.2); knowledge to understand factual conditions surrounding data governance in Fairview; and opinions and values questions to deepen understanding of actions and bring forth any underlying assumptions or ideological perspectives on data, which could explain competing concerns or tensions.

Semi-structured group interviews have the advantages of being inexpensive, data rich, flexible, stimulating to respondents, recall aiding, cumulative and elaborative (Fontana and Frey 1994; Nielsen et al. 2018). Group interviews focused on bringing forth dynamics or differences in perception, which normally would not be possible in individual interviews.

Date	Type	Source(s)	Duration
December 2018	Semi-structured group interview	Digitalization director and Information security coordinator	1 hour
December 2018	Semi-structured interview	IT manager	1 hour
December 2018	Semi-structured interview	Digitalization director	1 hour
December 2018	Semi-structured interview	Information security coordinator	1 hour
February 2019	Semi-structured interview	Information security coordinator	2 hours
February 2019	Semi-structured interview	Digitalization director	2 hours

February 2019	Semi-structured interview	IT manager	1 hour
April 2019	Semi-structured group interview	Digitalization consultant and business developer	2 hours
April 2019	Semi-structured interview	Information security coordinator	2 hours
April 2019	Semi-structured group interview	Data protection officer and Information security coordinator	2 hours

Table 8. Interviews conducted in the case study

4.3.1.2 Observations

Observations offered the opportunity to generate material, which was inaccessible through interviewing. It allowed the study of actions in real-time, in real-life organizational settings, by observing individuals 'doing things' (Mason 2002). Moreover, it allowed the observation of group dynamics within data ventures, where multiple practitioners were interacting to solve a problem. Additionally, it enabled access to perspectives and insights from individuals in the case organization, who otherwise might not have wished to participate in an interview or feel that the topic was beyond their everyday activities.

All observations are listed in Table 9. Throughout the empirical study, observations were made during everyday work practice (#1, #6, #7), team meetings (#2, #4, #8), presentations (#5, #9, #11), coordination meetings (#3, #10) and workshops (#12).

#	Date	Type	Source(s)	Duration
1	February 2019	Observation	Information security coordinator	2 hours
2	February 2019	Observation	Information security coordinator and Digitalization director	1 hour
3	February 2019	Observation	Two social workers, Foster care consultant, PPR[9] consultant, Digitalization director, IT developer and Information security coordinator	1,5 hours

[9] PPR stands for pedagogical and psychological advisor

4	February 2019	Observation	Digitalization director, three IT developers, Digitalization consultant, Business developer and Information Security Coordinator	2 hours
5	April 2019	Observation	Director of Children and Youth, Head of schools, Head of daycare, Head of management group, Head of PPR, Head of health services, Head of programs and Information security coordinator	1 hour
6	April 2019	Observation	Information security coordinator	2 hours
7	April 2019	Observation	Information security coordinator	2 hours
8	April 2019	Observation	Information security coordinator, Digitalization director and IT developer	1 hour
9	April 2019	Observation	Pediatric nurse, a physiotherapist, two special consultants, three social workers, PPR manager, the department secretary, Director of Children and Youth and Information security coordinator	1,5 hours
10	April 2019	Observation	Data protection officer and Information security coordinator	2 hours
11	May 2019	Observation	System owners from each department, Digitalization director, Information security coordinator and external consultant	2 hours
12	May 2019	Observation	System owners from each department, Digitalization director, Information security coordinator and external consultant	3,5 hours

Table 9. Observations in the case study

4.3.1.3 Documents and other materials

Studying documents and other materials can corroborate evidence from other sources and provide a greater level of detail than what can be achieved through interviews or

observations (Yin 2009). In longitudinal, processual case studies, archival records can offer retrospective insights on how the process unfolded before start of the empirical study (Van de Ven).

Throughout the empirical inquiry, multiple different document sources were collected (listed in Table 10). These offered insights into work practice during observations, offered a snap-shot view of decisions and informed greater detail in the empirical analysis.

Type	**Source(s)**	**#**
Document	Strategy documents	5
	PowerPoint-presentations	5
	Official principles and guidelines	5
	Internal e-mail correspondences	20
	Internal handbooks and rulebooks	5
	Data processing agreements and auditor statements	1
	Information security risk assessments and rapports	5
	Domain specific data protection regulations	1
IT artefact	Screenshots of domain IT system(s)	10
	Screenshots of PDF cleansing tool	3
	Prototype version of SecureDialogue	1
	Fairview municipality's website	1
Visual material	Pictures of the physical environment in the Fairview municipality building	10
	Pictures of the meeting screen in front of conference rooms	1

Table 10. Documents and other materials from the case study

4.3.1.4 Field notes

Spending time in the field offered opportunities for learning about the context, the case and the individuals through watercooler talk and over lunch with practitioners (Mason 2002). Most interactions here took the form of completely open-ended, conversational interviews (Patton 2002), which were unplanned and unrecorded, and mainly functioned as a way to establish rapport and trust with practitioners and get insights into actions and activities in informal settings. Observations, reflections and insights were captured in my field diary and subsequently also informed the empirical analysis.

4.3.2. CONCEIVING ANALYSIS FROM EMPIRICAL MATERIAL

In longitudinal process studies, most empirical analysis involves multiple iterations of induction, deduction and abduction over time (Van de Ven 2007). The themes laid out in Table 6 in section 3.3 functioned as preliminary devices for ordering and conceiving the empirical analysis. While this section suggest a clear progression and division in the activities of planning, ordering and conceiving empirical analysis, this was an iterative process which developed progressively over time. Each subsection highlights specific considerations that emerged in relation to specific activities.

4.3.2.1 Analytical approach

Empirical analysis covers a broad set of activities, ranging from sorting, organizing and indexing qualitative data, to developing holistic interpretations and producing visual diagrams or maps to represent event sequences (Mason 2002a) Several recognized approaches are available, ranging from more systematic to more creative. Cross-sectional, categorical indexing involves devising and applying a common set of indexing categories systematically and consistently across data (often referred to as "coding"), while non-cross-sectional data organization involves looking at discrete contexts and documenting something specific about these individual parts (Mason 2002a). Coding often carries connotations of being mechanistic, but may be understood as a process "that enables the researcher to identify meaningful data and set the stage for interpreting and drawing conclusions" (Coffey and Atkinson 1996, p. 27). The analytical approach for this dissertation involves elements from both approaches, as suggested by Mason (2002a, p. 166) and uses concepts and ideas derived from theory to consider patterns *across* data sources and explanations that emerge from non-cross-sectional patterns *within* parts of the empirical material.

Existing data governance research proved scarce in offering indexing categories as well as an appropriate theoretical framing (see Chapter 2). To facilitate better conditions for theorizing, guiding data analysis, and developing a contribution (Mathiassen 2017), a theoretical framing independent of data governance research was chosen (see Chapter 3). The chosen framing informed how the empirical analysis was approached. For the

original study of polycentric governance in self-organizing resource systems, examining how the organizing logic evolves implies both categorical and contextual understanding:

> ”I do not know what the structures of the situations were like before some appropriators in the mists of time began to experiment with various rules (…) They solved their problems the way that most individuals solve difficult and complex problems: as well as they were able, given the problems involved, the information they had, the tools they had to work with, the costs of various known options, and the resources at hand. I see my task as one of learning about the structures of the problems they faced and why the rules they adopted seem to work.” (Ostrom 1990, p. 56)

Thus, the process of analyzing empirical material was characterized by two types of activities; ordering the empirical material and conceptualizing the empirical analysis. For ordering the empirical material, a temporal sequence of incidents was established to get a sense of when what had happened (Van de Ven 2007). Next, indexing categories were developed from the theoretical framing and the empirical material was indexed according to specific instances that seemed to indicate these theoretical ideas (Mason 2002b). Next, a less structured and more holistic process followed, where several iterations of these two activities were repeated. This involved multiple rounds of experimentation with “slicing” the empirical data in different ways that would order the theoretical concepts in a comprehensible manner and conceive an accessible process narrative. Further details on these specific activities are elaborated in the following subsection.

The empirical analysis seeks to narrate how an organizing logic of polycentricity progressively evolves over time within Fairview municipality and enables the organization to devise data governance deliberate and emergently. Across four episodes derived from the empirical material, themes developed in the theoretical framing highlight how collective action is threatened, how polycentric governance is enacted to reduce impact of threats and mobilize collective participation, in which arenas actions occurs through zoom-in and zoom-out perspectives and how this enables practitioners primarily working with digitalization and information security to devise specific arrangements. To address the research question in a broader sense, data ventures as new action arenas and patterns of polycentric organizing are identified across the episodes and discussed jointly with extant literature to theorize how polycentric organizing can enable an organization to devise data governance arrangements in response to competing concerns for data use in the digital era (see Chapter 6).

4.3.2.2 From ordering empirical material to conceptualizing empirical analysis

It should be reiterated that this dissertation primarily seeks to engage in unfettered, blue ocean theorizing (Grover and Lyytinen 2015); to propose budding theoretical sketches that inform and stipulate further discussion and inquiry and to suggest relationships and connections that have previously been unsuspected, but have potential to change actions

and perspectives (Weick 1989). As noted in section 4.1.3, this does not exempt researchers from cogently explaining and motivating ideas, constructs or research design choices, for which reason this final subsection seeks to shed light on considerations informing the conception of the empirical analysis.

Each method of data collection yielded insight into different *incidents* (Van de Ven 2007, p. 218) which had occurred before my arrival, during my observation or was about to occur. Initial ordering activities focused on structuring the different insights I had obtained from data sources and arranging it in a chronological searchable format, since I had both archival records, retrospective accounts, direct observations, informal notes, transcriber interviews and various documents.

Categorical indexing (Mason 2002b) was used to get a handle on data and find a way into the empirical material. In this sense, the ordering of the empirical material was done "backwards", since the ordering of incidents in a temporal sequence usually constitutes the first step, but was done after a few preliminary readings of empirical material with the theoretical themes in mind.

After getting a sense of the theoretical concepts represented in the material, *temporal bracketing* was used to order empirically observed incidents into more abstract events (Van de Ven 2007, p. 220). An example could be how the empirically observed incidents; registering which data are collected in what systems, undertaking a security risk assessment, developing data processing agreements and saving these in one central system, together indicate the *event;* sketching boundaries of a common resource system. These events ultimately relate to the later theorized patterns of polycentric organizing (see Chapter 6).

After bracketing events, *zoom-in and zoom-out* (Nielsen et al. 2014) perspectives are used to consider how developments in the surrounding institutional environment that go beyond and overlap with organizational boundaries co-evolve with processes within Fairview. From the chosen theoretical framing, studying how data governance arrangements evolve calls for a perspective that is not restricted to one level of analysis, such as individuals, teams, departments or organizations, but instead specific pay attention to activities occurring in specific action situations (Ostrom 1990, 2005): "by zooming out, dynamics across the field and the range of players that are involved become visible, and by zooming in, dynamics within a specific organization (or even department)" (Nielsen et al. 2014, p. 180) become visible as actors devise arrangements.

While this dissertation undertakes careful empirical work to address the research question and explore concepts and ideas in an organizational setting, the process of interweaving such insights with loosely defined themes from theory was not objective, deductive, systematic or chronological, but unexpected, messy and imaginative. Theorizing in this dissertation involved leveraging familiar physical or linguistic objects, such as 'self-organizing resource systems' and 'data ventures', to highlight, clarify, enrich and enlighten

meaning about a fast-growing, constantly changing set of digital practices. In sum, theorizing in this dissertation was about "inventing explanations about things, not finding them" (Mintzberg 2005, p. 357).

Moving from observations and descriptions to explanations and theory requires a story (Van de Ven 2007). Narrating stories involves sequencing events in time with a progression of beginning, middle and end; it involves focal actors that tie events in the narrative together; a specific voice or viewpoint from which the story is told; an evaluative frame of reference to judge whether unfolding events are desirable or disadvantageous and; contextualization of events in time and place to enrichen understanding of events (Van de Ven 2007, pp. 223–224). Building theory in this way requires ingenuity and disciplined imagination (Weick 1989). In this sense, the structuring of the empirical analysis in the four episodes attempts to provide narrative progression, by detailing activities and dynamics in great detail, grouping thematically related events together in component plots, and by incorporating several quotes and observations from the empirical material to provide localized, detailed accounts as *structural tales* (Van Maanen 2011). The empirical analysis seeks to move from incidents to event sequences to episodes to develop a coherent process narrative, which in turn is meant to illustrate a theoretical sketch of how an organizing logic of polycentricity evolves and enables specific actions.

CHAPTER 5. EMPIRICAL ANALYSIS

5.1. OVERVIEW

The empirical analysis is structured according to four episodes identified across the empirical material and describes how practitioners in Fairview municipality progressively evolve polycentric governance for data use in practice. Each episode recounts specific problems that threatened collective action, how focal actors enacted polycentric governance, and how collective-choice arenas were brought into being to resolve issues, and shape congruent rules. Each episode also attends to how processes unfolding within Fairview co-evolved with activities in the surrounding environment, through zoom-in and zoom-out perspectives. Main highlights from the individual episodes are summarized at the end of each subsection, while the following provides a brief overview of the four episodes.

Episode #1 *Arranging for data as a collective resource* focused on early work to sketch the boundaries of a common data resource system in Fairview. The IT manager and the Digitalization director were focal actors and directed their attention to data governance as architecture principles for resolving a fragmented IT landscape. The episode concluded in May 2018, when instatement of GDPR had shifted attention to data as a collective resource in the organization.

Episode #2 *Experimenting with strategies for devising data governance* followed after the dust from GDPR had started to settle. The Digitalization director and a newly hired Information security coordinator were focal actors and began experimenting with different approaches for devising organization-wide data governance arrangements to ensure GDPR compliance. The episode concluded in December 2018, as perception of data governance had ultimately shifted from enforcing formal compliance to devising working rules.

Episode #3 *Activating collective participation* revolved around mobilizing support from individual practitioners in Fairview to participate in shaping rules for data use. The Information security coordinator was a focal actor and leveraged multiple organizational responses to address tensions between local work practices and collective concerns for data. The episode ended in March 2019 with the formulation of Fairview's first multilateral data governance arrangement for data sharing in coordination practices.

Episode #4 *Nesting data governance in layers* centered on combining efforts in multiple small-scale arrangements with large-scale supportive institutions. The Information security coordinator was a focal actor who progressively focused on enabling local practitioners to devise local rules for their particular context, building on mutual trust and reciprocity. The episode concluded in June 2019, as Fairview was actively enacting polycentric governance.

5.2. EPISODE #1: ARRANGING FOR DATA AS A COLLECTIVE RESOURCE

MARCH 2017-MAY 2018

In early 2017, the IT manager and the Digitalization director in Fairview municipality began work to arrange for municipal data as a collective resource. The national digitalization strategy (Agency for Digitisation 2016) which was published in May 2016 underscored public data as a valuable resource in improving the delivery of public services, enabling quicker case processing and supporting administration in general. While the strategy document acknowledged that the foundation for generating beforementioned value required greater data sharing, arrangements for doing so were not conceptualized as matters of devising data governance but of integrating IT architecture and using standardized data models (Agency for Digitisation 2016). This framing also shaped how Fairview municipality approached data as a resource at the outset of this episode:

> "we use architectural models to ensure we can have a more structured approach to [data] in our IT world and it is in this context that we introduce it (…) We must never neglect legacy in this because we have IT systems, where we don't have access to our own data, and if we want to access them, it will cost us a fortune, so we are looking forward instead of backwards" (IT manager, May 2017)

As the data resource was viewed through an IT architecture lens, governing data became about ensuring access and integration. This perspective consequently manifested in Fairview municipality's own digitalization and IT strategy, where visions for how to use data for generating value in public services again had an IT architecture flavor (elaborated later in section 5.2.4). Consequently, obstacles to organizing data were attributed to the absence of a data overview data across the organization. While the two mangers from IT/Digitalization were enthusiastic about the potential for data-centric technologies in a municipal context, they simultaneously considered it out of reach for their own organization, since it implied much higher IT architecture maturity than Fairview could support at the time:

> "I wish I could say we have a strategic approach to data overall, but we don't have that. We're trying to get it in now. Except for the research world, in practice it is actually a relatively new concept and it is exploding at a pace we have never seen before." (IT director, May 2017)

In summer 2017, the Digitalization director and the IT manager participated in the workshop series on data governance (see section 4.1). They were introduced to data governance as an approach to organizing data as a resource, with reference to a specific framework for devising data governance within an organization (Khatri and Brown 2010). Although recognizing the potential of data governance, the IT manager still saw

data governance as an element of IT architecture to ensure data integration between existing and future IT systems acquisitions:

> "The better we become at [data governance], and the more we work it into the way we buy and develop IT systems, the better that coherence [referenced in the framework] becomes. I think it's one of the keys to us getting there, and it's a long, hard path, but I really think it's critical" (IT manager, June 2017)

Little attention was paid to data governance for other purposes, even though the GDPR was already approved by the EU commission in April 2016 and set to enter into force two years later. Yet, by the end of the episode, this had changed. Several issues emerged as the two managers attempted to address data governance on an organization-wide scale. These issues indicated problems beyond IT architecture, and while they were still mostly addressed as such, the resulting data governance outcomes reflected that Fairview had seemingly evolved beyond just focusing on architecture.

5.2.1. COLLECTIVE ACTION THREATS

Three collective action threats shaped the first episode and mainly focused on little or no concern for data as a collective resource.

5.2.1.1 Little concern for data as a collective resource

When Fairview municipality started arranging for governing data as a collective resource, it remained an effort driven by the IT/Digitalization department. Since they perceived the effort as a problem of IT architecture, their motivations for devising data governance related to consolidating insights about and resolving lack of access to which data Fairview municipality had, where they were stored and who was responsible for them. Reversely, the current (non-existent) structure for organizing data was also attributed to a lack of overview:

> "Talking about structure and data governance (…) It's just not that organized, I can say that. We have a lot of data lying around in many places without us knowing it. We do not know even know the state of the data, or someone does, hopefully, but there is no collective overview" (IT manager, June 2017)

Despite having worked strategically with IT for many years, it had never been a priority in Fairview to think of data as a resource to be monitored and governed in a central place. There had been no attempt at charting or keeping track of organizational data, when developing or implementing new IT systems, but neither the IT director nor the Digitalization director showed much concern about this lack of knowledge at the time. Data governance was seen as prerequisite for exploring data-centric solutions, implying that if the IT/Digitalization department at least knew which data were located where, they could always find use for them later:

> "So, in relation to applying [data] broadly in contexts we have not seen before, which is actually where the issue is, it is not quite so problematic if we just make sure to compile data together, then we can experiment with putting some use to them later. But from what we saw, we must have it governed so that we know where [the data] are." (IT manager, June 2017)

For the IT manager, effective data governance could be devised without knowing what data were to be used for, which consequently left imperatives for doing so weak. Moreover, the current lack of overview, integration and access to data in Fairview was attributed to a lack of knowledge about why this was important, when Fairview first started implementing IT systems:

> "… one thing is the complexity of many systems, but something else is 40 years with systems that have been implemented at random […] It means that the structure you should have designed from the beginning, there was no knowledge of that time. It is not a complete mess, but you come from so many places that a unified approach to data, it has never been there. We sit on a gold mine of data and knowledge that we don't know we have" (IT manager, June 2017)

Incentives for governing data as a collective resource in its own right still remained insubstantial. Data governance was considered useful in the prospect of it providing a data overview, which was deemed desirable for its ostensible, but still unknown potentials for stimulating organizational value creation with data (in the future). Paradoxically, such an overview was not established in the past either, specifically because there was no knowledge about what data as a collective resource was to be used for and therefore no motivation to adopt a coordinated approach. These ideas also characterized how data was communicated as a collective resource to the organization in Fairview's own digitalization strategy. The IT manager and Digitalization director had lobbied local government managers and politicians to put strategic use of data on the agenda for the conception of their own municipal digitalization strategy for 2017-2020:

> "We will be working from a new digitization strategy, and data is actually one of the things we insisted should be on there, along with IoT and other things that are closely related. We went around talking to all the professional secretariats, but we are the only ones driving it; they are not motivated by it themselves" (IT manager, June 2017)

The final document indicated that having access to and ownership of data were prerogatives in themselves and that data were valuable, even if there was still no knowledge about their nature and potential use for the rest of the organization:

> "It can be difficult to know in advance which data may be useful in the future. That is why it is important, when entering into an agreement on acquisition of new systems, smart things or other units that collect data that Fairview

> Municipality secures ownership and access to the data generated, so they can be used if need be" (Digitalization and IT Strategy 2017-2020, Fairview Municipality, June 2017)

Consequently, incentives for data governance in Fairview remained closely tethered to IT architecture management, where the purpose was to ensure integration, access, overview and ownership of data. These incentives resonated with both the IT manager and the Digitalization director, who understood that such initiatives were valuable for the organization as a whole, because they would support business-oriented, data-centric solutions down the road. Albeit convincing for the two managers, they constituted weak incentives for governing data as a *collective* resource, seemingly not resonating with practitioners from other professional domains and thus posing a significant threat to mobilizing collective action for any subsequent data governance initiatives.

5.2.1.2 Weak incentives to adopt cooperating strategies for data governance

Beyond little concern for data as a collective resource, the IT manager and Digitalization director was dealing with another, deeper problem in devising and mobilizing support for lateral data governance arrangements. Operating from the Fairview model (see section 4.2), the organizing logic in Fairview built on local autonomy, decentralized decision-making, short communication paths and clear political influence, which were deeply embedded in the cultural fabric of Fairview as an organization:

> "I experience a significant challenge because I have been in an organization with 88,000 employees, and when someone said, "now, we run in that direction", then people more or less would run in that direction, whereas here, there is that way in which decisions are implemented, and it is very distinct and there is a lot of room for interpretation" (IT director, June 2017)

By extension, all the individual departments, secretariats and contractors in Fairview were afforded autonomy in purchasing new IT systems and while they could opt to seek advice and input from the IT department, this was not mandatory. From the 2016 national strategy (see section 4.2), the vision for a digital public sector specifically encouraged greater data sharing for developing more cohesive welfare services and enabling quicker case processing. Both of these would require substantial, centrally coordinated, cross-departmental governance arrangements, but the IT/Digitalization department knew they could not readily implore individual departments in Fairview to adopt such lateral governance arrangements:

> "We have formal authority to force architecture models through, of course we do. The challenge is, if what we do doesn't suit people, then at some point they will say 'forget it, we will do something else'" (IT manager, June 2017)

Even though the IT manager had formal authority to strictly enforce IT architecture principles, doing so would not necessarily discourage individual level actions or guarantee cooperation. The issue was further complicated by the way most data governance in Fairview was anchored in a variety of massive domain-oriented systems. These IT systems dictated fundamental data models, requirements and dimensions for data quality, responsibilities for data ownership, options and restrictions for data sharing and integrations with other IT systems. Some of these still counted legacy proprietary systems which had not been replaced or discontinued after the market for public IT development was deregulated in 2009 (see section 4.2).

The domain-oriented IT systems were not geared for sharing organizational data across functions but rather for supporting the specific nature of work and practice within individual municipal professions. While individual professions would have some incentive to coordinate development of new IT solutions between them, given the similarity of their work and opportunities for sharing best practices, this was not even the case in Fairview.

Especially primary schooling illustrated the nature and complexity of data governance. As sanctioned by the Fairview model, each individual school had negotiated their responsibilities directly with the city council and therefore had no formal obligation to cooperate either with the central IT/Digitalization department nor with other schools. Although 16 primary schools in the municipality had agreed on a new learning platform together with the IT manager, two schools had opted out. Pressuring the schools to cooperate through formal sanctions would yield no or even adverse incentives:

> "… then you can say, where is the domain secretariat in this, why don't they just put [the schools] in their place. Well, if they do, then the headmaster goes to the nearest politician, and says 'is it really true that we can't decide for ourselves', and then he answers, 'no, it isn't', and then follows a completely foolish discussion, seen from a data governance perspective. One we could never have anticipated" (IT director, June 2017)

The IT manager and Digitalization director knew they could not implore individual departments to adopt any general, lateral or even specific data governance arrangements without inviting conflict. The problem was further exacerbated by the way data governance arrangements were determined by and anchored in domain-oriented IT systems, since these systems were under the complete purview of individual contractors and departments to acquire and develop, as sanctioned by the Fairview model. Attempts by the IT and Digitalization department to conceive cross-functional or formal policies would likely be perceived as an infringement of domain experts' right to decide their own technology and therefore posed a substantial threat to collective cooperation and participation in organization-wide data governance initiatives.

5.2.1.3 High degree of heterogeneity among practitioners

As Fairview municipality started arranging data as a collective resource, it remained an effort driven by the IT and Digitalization department. Consequently, the IT manager and Digitalization director co-related what concept individual practitioners in Fairview had of data with their general understanding of digitalization and IT. Departments that were not working strategically with digitalization were considered to be less concerned with data:

> "We just had a talk with department for eldercare, because we really need to make a digitalization strategy, because they do not have [digitalization] at the forefront […]. The first meeting we have with them, they thought we were there to discuss which PCs they should have, and what phones to buy. And that was probably the last thing we were going to discuss. That doesn't mean there isn't a lot of good initiatives, but if you don't understand, why you have to incorporate digitalization (…) there is nothing you can do, if you don't have that awareness, and when you don't have that, you're not thinking about data" (IT manager, June 2017)

According to the IT manager, a lack of big picture thinking about digitalization in a given professional domain meant a lack of concern for data as a collective resource, where developing awareness on the matter would depend on developing an understanding of digitalization. Since departments in Fairview remained autonomous on the topic of IT acquisition and digitalization, high degrees of heterogeneity dominated across the organization:

> "There is a huge difference between the digital maturity, the skills and the understanding of what to do with these things and which types of data that is generated and on the whole, just working digitally. In some places, our focus is that we have to make sure we own data and they are stored safely, and everyone can relate to that. In other areas with higher digital maturity, they can already see some perspectives on how to use data a little more strategically, and are actually running data governance for their part of the organization, and so we have to assess the situation, and say where are we in this area and where do we start" (Digitalization director, June 2017)

If a department or profession was already working with digitalization in their core profession to a large extent, it meant they had greater concern for data as a resource. Since concerns for data were considered deeply intertwined with digital maturity in this way, any obstacles related to the former was magnified by obstacles experienced in the latter. To conceive of data as a collective resource, which needed to be governed through multiple, general and specific organizational arrangements would require an understanding of the purposes of digitalization, but this agenda was already met with misunderstanding and resistance by some:

> ”But the point is also that when it comes to the departments, they must understand what we are trying to achieve. That it is more than just “those computers” and making things more efficient. We have to get them on board with digitalization and say, if they are not, then it will just be fragments, where they each buy something here and there, and it will be such isolated sets of data, and even if we can keep them safely stored, they are not really creating value beyond because they have purchased such incompatible systems” (Digitalization director, June 2017)

According to the Digitalization director, mobilizing support for data governance was contingent on how well individual departments understood the purposes and benefits of digitalization beyond just the IT they acquired for their own department. Since digital maturity varied significantly, concerns for data as a collective resource were exceedingly asymmetric which posed a significant threat to collective participation, specifically for organization-wide data governance. Devising lateral arrangements across multiple maturity levels would either mean targeting the lowest common denominator, at the risk of leaving high maturity departments stagnant or targeting the desired ambition level, at the risk of leaving low maturity departments overwhelmed.

5.2.2. ENACTING POLYCENTRIC GOVERNANCE

At the workshop series in 2017, the IT manager and Digitalization director were presented with the data governance framework as a potential approach for organizing their data as a collective resource. They reacted to the normative assumptions underlying the framework by conceding that such an approach would be inherently limited in an organization like Fairview:

> “I think the model makes a lot of sense, but the challenge, of course, is the structuring and the applying it to everything and everyone. It is not going to happen, not in the sense where we say ‘we will do this now’.” (Digitalization director, June 2017)

Since Fairview was operating from its model of decentralized authority and decision-making, the two managers were acutely aware that expecting their entire municipal organization to suddenly adopt general, centrally defined data principles was not remotely feasible. They also pointed to inevitable ambiguities in terms like metadata and data quality, as well as the limitations of a centralized-decentralized dichotomy for organizing data governance in Fairview:

> “Just something like centralized versus decentralized, it's not unequivocal what that means. Not at all. Because for a school, decentralized means in their administration, where centralized means in the professional secretariat (…) The professional domain systems are so dominant, that you may have a number of domain systems that place decisions for data principles at the secretariat level, which for them would be considered the most centralized,

> but we as the IT department are not involved. Then we have some completely cross-functional IT systems, such as our payroll and financial system, where the data principles are completely centralized, so it is not clear-cut" (IT manager, June 2017)

In detailing why devising data governance from a normative framework would be problematic in Fairview, they simultaneously expressed the organizing logic in Fairview as one which did not resonate with centralized decision-making. Their experience with heterogeneity and autonomy of individual units in Fairview pointed to the importance of concentrating on actionable, small-scale solutions in order to incrementally effect change:

> "If this is going to work, then it must be made operational in some way, down to very specific initiatives, which are actionable, but grounded at the same time. This is the challenge with some of these concepts, like metadata, you would think that was a common term. It is really important to get it down into some relatively explicit models" (IT manager, June 2017)

They emphasized the role of localized problem-solving, but the Digitalization director also recognized that to mobilize collective action on an organization-wide scale, they would need to transform rules and norms at a deeper level than just the operational:

> "Once in a while we are forced to rise above operational level to have these discussions, because otherwise it will remain the isolated solutions and initiatives that set the direction (…) it will not create a revolution tomorrow where everyone is on board, but it is progressive understanding and it is about building more and more awareness about it" (Digitalization director, June 2017)

The IT manager and Digitalization director were focal actors in shaping the structure of incentives for data governance during this episode. Several small-scale, unrelated initiatives, like conceiving strategic IT architecture principles, lobbying for coordinated strategies in IT acquisition and engaging executive directors about the data governance framework involved little cost, but constituted important investments in arranging for data as a collective resource. The IT manager and the Digitalization director enacted polycentric governance incrementally throughout the episode, mostly by addressing smaller, second-order problems. They also engaged in sketching the early boundaries of a common data resource system in Fairview.

5.2.2.1 Defining boundaries of IT architecture

The IT manager was very vocal about realizing data governance through corresponding constructions in the IT architecture. He maintained that IT architecture was the underlying scaffolding supporting different information and technology needs in the different municipal domains but would never involve user input in its design:

> "IT architecture is something that lies behind the scenes, and then we have the IT system in front interacting with users. It takes a lot of user involvement to design the front, but never when it comes to architecture because they have no clue about that." (IT manager, June 2017)

His subsequent understanding was that governance arrangements for data as a collective resource would not be enacted as an organizational arrangement, but rather through IT architectural principles and other technological implementations. Although this attitude offered a very limited narrative for dealing with broader organizational complexities, the technical focus directed important attention to ensuring data collection, access, ownership and integration, which in turn constituted important groundwork in arranging for provision of data as a resource. His ambitions on behalf of the IT/Digitalization department to suppport data sharing and integration between hundreds of IT systems across autonomous units in Fairview resulted in the second-order benefit of establishing the early boundaries for a common "data resource system" in Fairview:

> "We have to be the torchbearers , and it does not emerge from our desire to be specifically business-oriented, it is purely a practical way to approach it. It's about building a platform that supports needs we do not know about yet, and we can't do that by asking the rest of the organization, we can only do that by exploring different directions. We try to be at the forefront and anticipate the situation" (IT manager, June 2017)

During this episode, concerns for data as a collective resource were asymmetric, heterogenous and mostly limited in Fairview overall (as described in the previous section). Yet, the IT manager did significant work to make data a collective resource for everyone in Fairview municipality, because fulfilling his ambitions for a more integrated IT architecture depended on broad acceptance and adherence to a newly defined set of architectural principles:

> "We are the ones, who are building it. The [data] models and the architecture, we are designing that. We have tried to interview some people from different positions in the organization and it is simply like when Ford was investigating the market for cars and all people wanted was a faster horse" (IT manager, June 2017)

The final principles reflected the early sketched boundaries for a collective data resource system. They included that new systems should be compatible with common platforms, emphasize cross-functionality, use open standards and become catalogued in a common tool Kitos, for creating an overview of contracts, interfaces, projects, GDPR compliance and the IT system portfolio.

5.2.2.2 Graduating sanctions through IT architecture principles

Polycentric governance was also enacted by introducing rules which allowed for progressively sanctioning non-compliance with the new architecture principles. During the workshop for executive group management in Fairview (see section 4.2.1), a common reaction from most managers was that the data governance framework made good sense, but was too advanced for their own organization, which lacked the requisite digital maturity. For the IT director in Fairview however, there was no clear distinction between devising data governance and mobilizing collective participation; those were both gradual intertwined steps. Therefore, he rejected the rational, all-or-nothing perspective implied by the framework:

> "We are not in a situation, where we can allow ourselves to say that we can't relate to it or we haven't come that far yet … again, it is this idea of all or nothing. This is not all or nothing." (IT manager, May 2017)

Rather than beginning with general ideas about the overall role of data in Fairview municipality, as prescribed by the framework, the IT manager knew this was an impossible position to start from, given heterogeneity of work. Instead, he focused on the individual IT systems, and one by one, assessed whether data governance arrangements existed, how they resonated with IT architecture principles and whether data was accessible:

> "We have to start incorporating [these rules], in a practical manner, from area to area, and it is a battle for every single IT system, even though it shouldn't be about IT systems, because it should be the other way around" (IT manager, June 2017)

Well aware that IT systems should support and not dictate data governance arrangements, he also knew it would remain the most practical approach in a decentral organization, which had no collective concern for data or IT. From this, he also considered IT architectural principles as the most viable way for progressively mobilizing collective participation in organization-wide data governance arrangements:

> "What will ensure that this works are the architectural models because there are no other ways around. Then it will be about getting more and more strict, and more and more adamant about whether or not people comply or can integrate with the models we have for how it should be. It sounds like IT is going to be bossy (…) but that is what is needed to carry this through, because if it is not made easy, and data are not available, then it will not happen" (IT manager, June 2017)

By focusing on preexisting data governance arrangements for IT systems and directing attention to gradually defining and enforcing stricter requirements for architectural

integration, the IT manager made it easier to achieve initial support and build forward momentum.

5.2.2.3 Mobilizing second-order collective action for digitalization

The two managers from IT and Digitalization inadvertently engaged in polycentric governance by addressing second and third-order problems related to collective action for data governance. Understanding data as a phenomenon in itself was far away from the reality of most non-IT practitioners in Fairview. Instead of directly devising large-scale arrangements, they focused on reshaping the structure of incentives for data governance by addressing digitalization within individual domains, in a way it made sense for the individual practitioners:

> "We should not sell it as efficiency. We should shift focus to look at it from the user side, because all the efficiency initiatives that we experience from inside and out, have provided some curious solutions from a citizen's perspective. It makes no sense whatsoever. That is the mindset we are working towards now, and it gives a fun "aha" effect for those that interact with citizens all the time, because you point it out to them, and suddenly it dawns on them, that this is not actually what we have been doing" (IT manager, June 2017)

A common way of mobilizing support for initiatives in Fairview that required broad participation from heterogenous units with diverging interests, was to reach for the lowest common denominators: efficiency improvements and cutting resources. Yet, most of the practitioners with little concern for data as a collective resource were often those closest to the citizens. The IT manager therefore saw digitalization as means for improving how citizens meet and interact with local government, where appropriate data governance arrangements constituted a necessary element in delivering better welfare services. By addressing a different, but related issue, collective interest and support for data governance could be tentatively formed.

Since most organizing was done behind the scenes by the two managers from IT/Digitalization, they were acutely aware of their own bias in working cross-functionally with technology. As part of the Finance, IT and Innovation administrative department, they were placed centrally, while their core responsibility was to think broadly and support the entire organization. For the rest of Fairview, this was not the case, so they were careful about taking into consideration that the further away a municipal practitioner was placed from the central administration, the less meaningful data governance arrangements seemed:

> "The further we get out to where people are close to the citizen and operations, the less meaningful they experience [data governance]. So, for

> example, there is a KLE record taxonomy[10] you use in the journaling system, and some centrally placed secretariat people who assign numbers to cases find it incredibly meaningful and can see the value in it, but as soon as you take a step further out, to the social worker or a teacher, they cannot see the value at all, and then we may sit here and say it's smart (…) but in their everyday work, it takes up so little attention" (Digitalization director, June 2017)

While the IT manager and the Digitalization director were focal actors in this episode, they also worked to establish second-order collective action and participation in shaping governance arrangements, by addressing second-order problems, such as the incentives for digitalization and achieving initial support for that.

5.2.3. ZOOMING OUT

Central developments in Fairview were also shaped by other processes unfolding in multiple national and international arenas. The national digitalization strategy set high ambitions for use of data in the public sector in general, but this was also followed by a joint municipal digitalization strategy, emphasizing specifically the role of local government in achieving the national goals. Amongst other goals, this strategy implored municipalities to standardize data, facilitate data sharing, both internally and with other public sector organizations, conceive evidence-based initiatives and release open data (Local Government Denmark 2015). Fairview's own digitalization strategy specifically stated that the purpose was not only to provide a common direction for digitalization initiatives in Fairview, but also to support achievement of both the national and municipal strategies.

Throughout the episode, no other collection of incidents intertwined with unfolding issues in Fairview in the way that the conception and instatement of the European General Data Protection Regulation (GDPR) did. While the regulation passed already in 2016, it only began materializing in Fairview as episode #1 was nearing its end. The regulation came under heavy scrutiny by popular media, which predicted no organization would be ready by the time and inflated fears about the massive penalties fined for non-compliance. Although the main substance of directives in the regulation were similar to previous directives (see section 4.2 for further details on GDPR), doubts and mass hype characterized the period before the regulation was set to enter into force by May 2018.

Since the regulation primarily concerned private, personal and sensitive data, it had major implications for the way data governance evolved in Fairview and Danish municipalities

[10] KLE refers to a records management taxonomy developed by Local Government Denmark which seeks to connect municipal responsibilities with corresponding obligations mandated in the law by categorizing cases in an intricate numbering system

in general. Although collection of these data in municipalities were sanctioned under purview of Danish law, no internal structures existed for documenting how these data were treated, processed or protected. An entirely new industry spurred around data protection, consultancy firms charged heavy sums for helping organizations become compliant before the implementation date, dedicated IT systems were developed for automating GDPR compliance and a wealth of online courses were developed and mandated for employees in any organization dealing with GDPR related data. The Danish Data Protection Agency, which had existed since 1979 experienced 150% increase in their activities (see section 4.2), because many organizations were bewildered about how to implement directives.

These developments had lasting impact on how data governance was approached and devised in Fairview from then on. A central implication of the GDPR was a shift in understanding of data as a collective resource, from an IT architecture issue to a matter of data protection and information security. In extension, the Local Government Denmark association released extensive material and hosted multiple courses on how to implement the ISO27001 standard for information security to remain compliant with the directive. As a result, consequent data governance arrangements in Fairview municipality were conceived in the context of this standard. Despite all the efforts, a survey conducted in May amongst 86 municipalities showed that 41 of them were not compliant by the time the directive entered into force (HK, 2018).

Although municipalities constituted a unique industry, given that there was no competition to the services they supplied, they were not unaffected by field-level pressures. As the attention to data exploded in other industries, it inevitably affected Fairview too:

> "Municipalities should not be seen as something that is isolated from what is happening in the rest of society, and there is a development as in all other industries. Data use is increasing in all sectors, and some are better at using data (…) We have no competitors in the services we provide, so the inertia caused by being a monopoly might mean that we act a bit slowly by comparison, (…) but the pressure comes from other sides, from the EU, from Parliament" (IT manager, June 2017)

What transpired in Fairview during the first episode was mostly characterized by responding to institutional pressures from larger settings.

5.2.4. EPISODE SUMMARY

The first episode *Arranging for data as a collective resource* focused on how two focal actors, the IT manager and Digitalization director in Fairview municipality began to arrange for provision of data as a collective resource. At the outset of the episode, Fairview was not working deliberately with data governance, data was not seen as a collective resource, but rather as an IT asset and most rules for governing data were "invisible", meaning they

were either implied in domain specific regulations or entangled in the design of IT systems. An IT architecture perspective had left weak incentives for the rest of the organization to consider data a collective resource, while the autonomy afforded by Fairview's operating model provided left weak incentives to adopt coordinated among highly diverse municipal domains with heterogenous concerns for data in general.

Several incidents signaled the end of episode #1. The IT manager ultimately left Fairview municipality in May 2018 and the Digitalization director consequently absorbed his responsibilities until a replacement could be found. Additionally, the implementation deadline for GDPR had passed, also in May 2018, which changed the pace in devising data governance arrangements going forward. GDPR brought data to the forefront in Fairview. Where incentives for data governance had previously been clear for IT practitioners, but murky for the rest of the organization, the new directive shaped conversations around data privacy, protection, ethics, and security, overshadowing previous technical concerns for integration, access and sharing. At the end of May 2018, Fairview had consequently begun arranging for provision of data as a collective resource.

Polycentric governance was enacted in several ways. Rather than lobbying directly for the importance of organization-wide data governance, the IT manager and the Digitalization director made several small-scale, low-cost investments in establishing a common, integrated IT architecture, which inadvertently established the initial boundaries for a common data resource system in Fairview. In doing so, the two managers effectively changed the structure of incentives in which future data governance arrangements would be progressively devised and mobilized in Fairview. Both the IT manager and the Digitalization director paid specific attention to rendering data governance meaningful for practitioners with frequent citizen interaction, but overall acknowledged how a centralized, top-down approach to devising data governance would never work in Fairview.

5.2.4.1 Highlights from Episode #1:

- The IT manager and the Digitalization director were focal actors in arranging for provision of data, which inevitably shaped early incentives for data governance as distinct technical problem.
- Dominant organizing logic of local autonomy and decentralized decision-making resulted in high degrees of heterogeneity among practitioners and thus weak concern for data as a collective resource.
- Technical focus directs attention to a fragmented IT architecture and a series of architecture principles, which inadvertently sketches the early material boundaries of common data resource system in Fairview.
- Focal actors created small-scale change in structure of incentives by focusing on addressing second-order problems related to digitalization and digital maturity.

- Focal actors accepted the inadequacy of top-down, centralized models for devising data governance arrangements in Fairview and adopted a practical, incremental approach to shaping rules instead

5.3. EPISODE #2: EXPERIMENTING WITH STRATEGIES FOR DEVISING DATA GOVERNANCE

MAY 2018-DECEMBER 2018

By May 2018, the digitalization director did not immediately link GDPR initiatives with data governance in the sense it was defined during the initial workshop and interviews. While significant work had been accomplished on developing risk assessments for IT systems and data processing agreements in preparing for instatement of GDPR, the Digitalization director considered data governance to be stagnating and lacking a proper hook to propel it forward in Fairview. When a new IT manager was hired and onboarded in June 2018, and the Digitalization director had to separate their responsibilities, the way data protection had been implemented was taken up for revision:

> "when our IT manager left in April, the responsibility for implementing the personal data regulation was taken up for reassessment because it had until this point been primarily with him. I had of course worked with him on some of it (…) but when he stopped and we were looking to hire a new IT manager, we tried to look at it again and said, all this work surrounding security, also the organizational part, is it naturally an IT responsibility? And then we really chose to say, well the cyberphysical security around our entire infrastructure, firewalls, all that, network and so on, it still lies in IT, but the work with the organizational implementation of the data protection regulation, it moved on to me, and eventually included the hiring of an information security coordinator" (Digitalization director, December 2018)

As the Digitalization director had reenvisioned the division of responsibilities between himself and the new IT manager, he also saw the need for creating a permanent position for an Information security coordinator. Instead of lumping concerns for data governance together as a distinct work assignment for the IT manager, as it had previously been, data governance was split into concerns for technological cybersecurity, organizational data governance implementation and information security coordination, which were divided between the three positions of IT manager, Digitalization director and Information security coordinator. These three were also focal actors in episode #2, where they began experimenting with different ways of devising data governance.

At the outset of the episode, the implementation date for GDPR had just recently passed, which meant that most data governance arrangements related to formal compliance. Yet, these efforts also seemed to have some benefits beyond just compliance:

> "I'm becoming more and more fond of the GDPR. It has given me the authority to compel some of our suppliers to comply with certain agreements" (IT manager, December 2018)

When the newly created position of Information security coordinator was filled in August 2018, the main responsibilities of the role included performing risk assessments on all IT systems, reviewing or writing data processing agreements for all IT systems, obtaining auditor statements[11] on all data processing agreements, as well as conducting mandated education for all personnel on the regulation and promoting general awareness about data protection in Fairview. Although GDPR was an EU mandated legal regulation, with unprecentedly harsh sanctions for violation, there was no method or straightforward way to implement it. The regulation specifically required extensive documentation demonstrating compliance, but no templates, standards or models were available. The ISO27001 standard for information security was identified as the closest formal standard, and most municipalities, including Fairview, decided to structure their implementation according to this.

In working with instatement of GDPR, Fairview mapped their organizational data in elaborate overviews and developed effective processes for monitoring and sanctioning non-compliance with the new data protection rules within the organization. At the outset of the episode, the Digitalization director and the Information security coordinator did not immediately recognize the work they were doing in relation to GDPR also constituted devising data governance. For them, the two were separate. As these rules were still clearly devised and imposed from the outside, the actual data governance arrangements were met with substantial resistance from other practitioners within Fairview.

5.3.1. COLLECTIVE ACTION THREATS

Where collective action in the first episode was threatened by weak or adverse incentives for considering data as a collective resource and adopting coordinated strategies to govern it, the harsh sanctions involved in not complying with GDPR momentarily reduced the impact of these issues. Instead, they were replaced by threats resulting from external pressure for both complying and demonstrating compliance during this episode.

5.3.1.1 Internal resistance to rapid exogenous changes

Although Fairview municipality had adopted many external directives, strategies and approaches in the past, with little or manageable opposition, the necessary change in rules prescribed by GDPR were so fundamental that it momentarily destabilized existing governance arrangements in Fairview. The requirements seemed both abstract, and extremely restrictive, since the sanctions for non-compliance were so harsh. Given that no straightforward implementation existed, practitioners became overly careful and frustrated:

[11] An auditor statement is an official report written by a lawyer, which reviews and certifies that the data processing agreement for a given IT system complies with the regulation

> "What I experience is very much the perception 'we aren't allowed to do anything at all, we can't even wiggle our ears' (…) overcautiousness and as a nuisance that is only put in the world to prevent people from doing their job" (Information security coordinator, December 2018)

Few non-IT practitioners in Fairview had any concept of data prior to this regulation, and many felt it prevented them from properly performing their everyday tasks. Those who had shaped their treatment of data to support individual routines and assignments, where no major professional IT systems dictated data governance, were uncertain and confused:

> "These workflows involving 'where are you supposed to record which data', specifically linked to the whole Microsoft Outlook package, with both e-mail and calendar and so on... It's something we get a lot of questions about and people, they have a hard time complying with the rules we set up, because they are confronted with sensitive or confidential data constantly, and have to make sure they delete it everywhere, after documenting them in another system. It really is an area where I find that people have a hard time with it" (Information security coordinator, December 2018)

The directives in GDPR were not only abstract, but also defined in an exogenous setting far removed from the norms and values in Fairview. Interpreting and implementing rules for their own work practices were therefore considered a hard challenge for practitioners, who had to translate abstract rules to action. Awareness and individual understanding were seen as crucial:

> "Awareness is central to capturing the small, informal things, and initiatives that promote protection, and rhetoric from immediate managers who emphasize the importance. We also have a gut feeling from speaking to other municipalities about what goes wrong" (IT manager, December 2018)

Although most of the work done by the IT manager, the Digitalization director and the Information security coordinator involved creating formal, written documentation, the individual habits of practitioners in Fairview could not be documented and improved on in the same way. The resulting pressure from translating and implementing abstract, normative rules in an environment where violation were harshly sanctioned posed a significant threat to collective participation in new data governance arrangements.

5.3.1.1 External scrutiny of behavior

During the time leading up to the implementation date, GDPR had received extensive media coverage (see section 5.3.3) and brought the issue of data privacy to the forefront with citizens. Attitudes towards data from citizens shifted quickly from being a secondary, but necessary by-product of having a digitally mature public sector to becoming an asset, they demanded be protected and treated responsibly:

> "Now they are referred to as the citizen's property, something we borrow and therefore must take good care of. It is not just something the municipality owns, which is a huge change in perception. In the past, people did not talk about data, perhaps nothing more than being able to do their job. And now there is attention to the fact that it is valuable, and discussions about ethics, fear and respect for the citizen's right to be private. It was not seen before. It is no longer about 'what can you do' but 'what should you do'" (IT manager, December 2018)

Where a lack of concern for data as a collective resource had previously threatened collective action, there was now intense scrutiny and attention, specifically from citizens, who wanted to know their data was not being illegally shared or repurposed. The regulation had succeeded in directing attention to a previously unacknowledged stakeholder, the data subject, which shifted the citizen perspective almost immediately. The central aim of developing GDPR, as stated by the EU (see section 4.2) was to let the people about which data concerns control who can process it and for what. As municipal practitioners in Fairview struggled with adhering to the many rules and interpreting the grey areas in their own work practices, citizens became overtly vigilant and attentive to how their data was governed in the municipality. Throughout the episode, Fairview experienced that multiple complaints were filed directly to the national Data Protection Agency about behavior which was neither considered in violation nor covered by the regulation at all.

Massive attention from broader settings on the role of the data subject in GDPR increased scrutiny on nearly all data governance in Fairview. Not only did practitioners spend significant time and resources interpreting the directives for themselves, and being overly careful to avoid massive fines, but they also had to deal with local complaints and formal audits. The three central actors in Fairview, the IT manager, the Digitalization director and the Information security coordinator therefore had to devise further governance arrangements, not directly to comply with GDPR, but to satisfy citizen concerns, which posed a threat to collective participation from municipal practitioners, who felt they were under surveillance.

5.3.2. ENACTING POLYCENTRIC GOVERNANCE

A central prerogative of GDPR was not only mandating that data be treated under purview of specific lawful bases, but also that organizations were able to document they were doing so. In Fairview, most of the time and resources dedicated to instating GDPR was spent on formal documentation to demonstrate how data was collected, processed, exposed to major risks and a wealth of other requirements. Failure to document compliance was sanctioned just as hardly as actually violating the data subject's rights. Therefore, significant work was done by the IT manager, the Digitalization director and the Information security coordinator to establish clear boundaries of the common data resource system, and on defining who had rights to access and use which data in line with the directives.

In implementing the regulation, the three actors inadvertently enacted intricate monitoring and sanctioning practices within Fairview:

> "People become in doubt about something and of course, sometimes, they are told 'yes of course you can do that', there is nothing there and then they are happy and satisfied. But just the fact that they ask, about all sort of things, I keep a record of it. It has become part of my job to keep track of questions" (Information security coordinator, December 2018)

As the Information security coordinator constituted the only point of contact in which practitioners felt they could ask questions about GDPR, it offered a cheap way of learning about which rules caused trouble and required further attention.

Since GDPR was not a standard, but legislation, there were no formal controls or requirements to guide its implementation and assess progress. Instead, individual organizations were solely responsible for devising the necessary governance arrangements to comply with the directives in their specific industry and organization. As the second episode progressed, the Information security coordinator had actively leveraged this mandated right to freely organize by trying out different strategies for identifying problematic areas, devising effective, situated data governance arrangements and then mobilizing collective participation. As a result, she experimented with a new form of action arena, the data venture, and learned about previously unavailable opportunities for action and collaboration outside preexisting organizational structures.

The IT manager, the Digitalization director and the Information security coordinator were focal actors in devising data governance arrangements during this episode. Although these processes were motivated by GDPR implementation, the three still enacted polycentric governance by defining boundaries of the data resource system, instating intricate monitoring and sanctioning practices, leveraging their rights to organize and by exploring an entirely new action arena; the data venture. This type of action arena was tried out by the end of the episode in order to resolve competing concerns for specific data, which were not formally governed by the GDPR, but heavily criticized by citizens, who demanded appropriate data governance arrangements be developed.

5.3.2.1 Defining boundaries and access to data as a collective resource

While the previous IT manager had taken small, but important steps in sketching the boundaries for a common data resource system in Fairview through IT architecture principles, the Digitalization director continued this work as part of GDPR implementation. He managed to map a majority of the IT systems in the organization, achieving the coveted, but difficult overview, by leveraging an existing way of organizing:

> "All this mapping in relation to our IT systems. There are data processor agreements, which were followed up with auditor's declarations, if that was necessary to have registered in relation to the data in the system; what exactly

> is recorded in the individual systems, what are the related domain areas and what staff uses the different systems. We have a map of system administrators, or they are not called that, because then they are confused with system owners, but we call them Kitos responsible, because Kitos is the system where we register all our systems. There we have someone from each domain for each department, who is responsible for registering these things." (Digitalization director December 2018)

Rather than reviewing each IT system on his own to assess what data were collected, he expanded an existing practice of registering all domain systems in a common system, Kitos. Since Kitos was an open source solution developed by the municipal-driven community OS2, the developers had expanded functionality for registering whether IT systems involved GDPR governed data and for storing related data processing agreements, risk assessments and auditor statements. For each IT system, Kitos also provided an overview of user access rights as they pertained to different organizational roles. Besides revealing multiple oversights, the overview also reflected how a lax and precipitous attitude had previously characterized how access rights were designated in Fairview:

> "… it was more laissez-faire, more based on what people wanted to have access to. There were many, who had a knee-jerk reaction and just automatically thought they should have access to everything. I definitely think that the communication and discourse around working with personal data, it has made things more rigorous, saying it is something we need to watch out for "(Digitalization director, December 2018)

Previously, access to IT systems had been designated fluidly, without a clear purpose, which was now mandated under GDPR. In establishing boundaries for the data resources system, the digitalization director also learned about how to distribute and monitor access rights. Although it was not explicitly recognized as such during the episode, this work was important in shaping the way data governance arrangements, which were not explicitly informed by GDPR, were devised:

> "But now in relation to our work in a Digitalization department, we can clearly see that there are some very central connections, in relation to getting the data defined and getting the organization mapped, saying these data belong here (…) and these data domains need to go here, and we have the opportunity to support a whole lot of other processes in a much smarter way by having control of the organization and what data needs to go where" (Digitalization director, December 2018)

Implementing GDPR constituted a second-order problem in devising data governance, but the incentives for chartering organizational data in becoming compliant provided surprisingly valuable, first-order benefits, as the Digitalization director could now make

use of the same overview to support other initiatives related to data as a collective resource.

5.3.2.2 Arranging monitoring and sanctioning practices

Harsh sanctions for not being able to document appropriate data governance arrangements supporting GDPR necessitated corresponding ways of monitoring whether practitioners remained compliant. No organizational roles and responsibilities were officially defined for how to undertake this task, except for one, namely the position of the Data Protection Officer (DPO). Reporting to the highest level of management, the role of the DPO was to ensure their organization remained aware of and educated in all relevant GDPR obligations, to conduct audits proactively and to function as the official liaison between the public and the organization on matters of data protection and privacy.

In hiring for this position, Fairview considered different options, before they finally decided on a model with an external lawyer on a retainer of six hours per month, as opposed to an internal legal advisor. This meant that everyday monitoring activities could not be overseen by the DPO, but instead were left to the Information security coordinator, who would have deeper knowledge about Fairview and its practices and therefore a better judgement of whether certain arrangements were permitted. Yet, as the data protection regulation had painted such a grim picture of violation and threatened with extremely harsh sanctions, practitioners in Fairview were anxious to make sure they remained compliant. They demonstrated informal compliance by consulting with the Information security coordinator:

> "We can tell by the fact that more and more are coming to me with questions, I mean of course they now have a specific person to ask the questions, but there is an ongoing stream of questions directed at me, about everything, such as: we have to take pictures and use them in our pedagogical work, how long can we keep them on our phone, how do we make a consent form, all sorts of possible and impossible inquiries "(Information security coordinator, December 2018)

Instead of actively seeking out practitioners, auditing their practices and monitoring their behavior, the Information security coordinator inexpensively obtained information about what practitioners were dealing with through their questions and proactively helped to resolve potential issues before a violation occurred. In turn, when a concern had been voiced numerous times, she decided whether a formal arrangement should be devised to resolve it. The Information security coordinator was also not blind to the significant confidence required for practitioners to entrust her with their doubts and questions in this manner:

> "We succeeded in creating a trust (…) One thing is to make people understand, that they have to report it, if they've made a mistake, and then

> we will take it from there together. But I actually think we succeeded in getting it conveyed in such a way that people also do it, because there is a confidence that this is a problem we must solve together; it is not about us going out and holding it over someone's head." (Information security coordinator, December 2018)

This informal approach to monitoring compliance was not considered controlling or undesirable, but rather as a meaningful exchange, where practitioners could safely voice their concerns and the Information security coordinator could inexpensively learn about compliance. In extension of this trust, practitioners also felt confident enough to report their own violations, without fear of uncomfortable repercussions:

> "I actually think we have succeeded, so that there is not a fear but a trust that we will help them (…). because it's a bit special what you do when you make a mistake, and you have to contact some employee in the central administration who needs to fill out forms and report it to the Data Protection Agency (…) one is essentially out doing self-incriminating work by saying 'I have really made a mistake', but the hurdle, I think it seems we have moved beyond it. We do a lot to remain proper in dialogue and aware of how we handle the inquiries that come in, so people do not become afraid to approach us again"(Information security coordinator, December 2018)

As practitioners were not only open for sharing doubts and questions, but also for reporting their own violations, these monitoring practices allowed for inexpensively graduating sanctions for non-compliance. Seemingly, this was broadly known and practiced in Fairview:

> "We have really succeeded in dispersing this trust widely and we get security incidents reported from everywhere in the organization and I think that is a good indicator that we have actually succeeded in getting that part communicated." (Digitalization director, December 2018)

Relations of trust were not only important for directing questions and doubts, but also for mobilizing participation in collective monitoring and sanctioning practices. Since incident reports were received from many different departments, the rules for self-reporting were seemingly widely known and followed by practitioners in Fairview. A corresponding large-scale arrangement in the form of an overview of risk and impact assessments were developed to complement the collective monitoring practices:

> "Each system has an overview of impact assessments, which consider a number of different parameters, such as what are the consequences for personal data security, if personal data is compromised, will it be available to others and what are the consequences of that (…) then there is also a focus on what happens if the data is not valid, what consequences are there, how critical is it, and then again how critical is it if we do not have access to the

> information contained in the system" (Digitalization director, December 2018)

IT systems containing personal or sensitive data with high impact and risk assessments were consequently prioritized in the process of reviewing data processing agreements and auditing these.

5.3.2.1 Actively leveraging rights to organize

Frustrations proliferated initially about the lack of formal requirements for implementing GDPR in Fairview. As the Information security coordinator was hired in August 2018, she began searching for formal approaches which could support the necessary processes, particularly for developing organization-wide overviews and data governance arrangements:

> "it's not optimal (…) many approaches have been developed to make these registrations. Certain law firms have also developed something, others are using home-spun spreadsheets. There are no form requirements, so you can do it in a lot of ways, and there are advantages and disadvantages with such an overview, because there is so much information you want to stuff in there and sooner or later, it no longer gives an overview" (Information security coordinator, December 2018)

Multiple options were available for overseeing compliance with GDPR, where the Information security coordinator had access to learn about practices for tackling related implementation challenges from other organizations and municipalities. Eventually, Local Government Denmark chose the ISO/IEC 27001 standard as inspiration for devising functions, roles and management for information security in a municipality. The purpose was not to become certified in the standard, but to use its structure to construct data governance arrangements which would then be considered sufficient to comply with the GDPR. Therefore, the association released a template presentation with an overview of how the municipalities could adopt core requirements for information security from the standard.

Fairview also decided to pursue this path, and while it gave the impression that formal arrangements were devised to ensure compliance, the standardized form was hard to implement in practice. The standard as modified by the municipal association specified the designation of an interdisciplinary Information Security Committee, ideally placed at top management levels to set goals and ensure information security was realized and complied with in the organization. While the Information security coordinator had succeeded in placing this responsibility with the executive management group, it also slowed progress:

> "It is very well done that we have been able to push it all the way up there, because then it has a certain legitimacy. The challenge is however that they

> already have a thousand other things to think about and that they do not necessarily know exactly what [information security] is about" (Information security coordinator, December 2018)

In effect, instating formal arrangements changed very little in practice, but rather than increasing attention to normative models, the Information security coordinator actively leveraged the freedom to organize:

> "There is no official rule book, where you can look up how to handle the entry of sensitive personal data in a calendar invitation in Outlook. You simply have to invent a new level" (Information security coordinator December 2018)

Given the high levels of abstraction implied by the GDPR, the Information security coordinator experimented with creating appropriate intermediate 'levels' for data governance arrangements, which could embrace compliance with strict regulations and simultaneously make sense in very localized work practices. Leveraging the right to freely organize in inventing these levels resonated better with the norms and values of Fairview, where autonomy and local-decision making were deeply embedded in the cultural fabric of the organization:

> "There is a lot of local self-government in the Fairview model, so even if you are a contract holder (…) they have goals and different things they have to comply with and deliver on, but they have always had a lot of autonomy (…) They perceive themselves as independent organizations, and of course they are too, but they have had to figure this out for themselves. They are not in the habit of consulting central principles for how to do things" (Information security coordinator, December 2018)

Fairview was characterized by individual units' rights to organize their responsibilities in the way they saw fit and the Information security coordinator acknowledged that any data governance arrangements needed to be 'cut' differently than in the usual central-decentral conception. Although contractors were keen to ask individual questions or report standalone violations with the central administration, they were unlikely to follow standard arrangements far removed from their own reality, since they were used to deciding for themselves. Learning about this condition signaled a small shift in perception for the coordinator but had significant implications for how she approached devising arrangements going forward and for mobilizing collective participation in episode 3.

5.3.2.2 Exploring a new action arena

As the Information security coordinator found that going directly to conceiving formal, complex institutions for data governance was ineffective and had little effect on actions, she also understood that mobilizing collective participation for organization-wide arrangements was not a trivial task:

> "They have different routines and everyday lives, they have different systems and different processes, so it becomes difficult to say something general that isn't too trivial like 'you have to take care of the citizens' data', which becomes empty platitudes that they have already heard countless of times, but they still lack actionable guidelines, like when should I do what and how"(Information security coordinator, December 2018)

Formal arrangements were effective in producing documentation and demonstrating compliance, but essentially ineffective in establishing the necessary data protection practices. Practitioners found it impossible to translate and transfer rules to their own everyday behavior and the Information security coordinator knew it would require deep appreciation for local norms and individual practices to anchor arrangements in organizational reality:

> "I have to enter reality, if you know what I mean. I have to meet the end users, because it is no use, not in any organization, that you remain comfortably seated in the ivory tower and send out e-mails, thinking 'well, now I have said it, so now they know what to do'." (Information security coordinator, December 2018)

Instead, the coordinator was prepared to tackle issues that were not immediately relevant for the organization as a whole, but represented urgent, competing concerns in smaller, local units. Arrangements of this kind were unprecedented in Fairview at the time. Individual units contacted the IT department for help with IT acquisition, and while requirements and optimal solutions varied between domains, this process was formalized, with clear definition of roles, responsibilities and expected outcomes for involved parties. What the information security coordinator conceived however was a new form of action arena, where roles and responsibilities were blurred, and the goal was to achieve mutual understanding and accommodation with no clear end in view:

> "It has to be brokered much closer to the context. You have to physically show up, you have to be ready to look at the specifics of their everyday life, and it might be, that overall they just have to do what everyone else does, but you have to tell them that in a simple manner as they ask 'when I sit here, with this task, in this system, what then, what applies?' You must place it in that context." (Information security coordinator, December 2018)

These ideas formed the basis for making use of a new type of action arena in Fairview; the data venture[12]. While the information security coordinator did not explicitly use the term, the description of her practical approach to establishing a mutual space in the local context, where devising data governance was accomplished through mutual understanding and collaboration embodied what the data venture concept was about.

[12] See section 2.3 for further explanation of the data venture concept in theory and practice

The coordinator deliberately constructed locally anchored, temporary collective-choice arenas, where practitioners could receive help and guidance with the specific tensions they experienced as a result of the new, general rules for collecting and processing data and negotiate reasonable resolutions for how to handle these tensions in their own local work practices. Even if the outcome of the data venture in a broad perspective was that practitioners ended up implementing the same rules as everyone else, the resolution had been negotiated in response to their specific experiences and therefore anchored abstract rules in their own local context:

> "It's a balancing act, because we can't hold everyone's hand and address individually every single employee, but those accommodations work. As soon as they move away from the very general, that is, just repeating the directives, as soon as we go beyond that, it will be difficult, so it must be very tangible for each domain. It is difficult to find something in between, to go from the very general to the very specific" (Information security coordinator, December 2018)

While data ventures developed as a viable action arena for anchoring general GPDR rules in local departments and teams, the Information security coordinator leveraged these initial experiences in tackling problems with devising organization-wide arrangements. The need for managing a data venture, which spanned across hierarchical levels and domains, began to materialize in response to the competing concerns involved in what data was allowed to be recorded in calendar invites:

> "We are working our way towards one related to our calendar, where there have been very different practices surrounding what you enter. There are many things to consider. There is nowhere we can look up 'what are you allowed to write in your Outlook calendar invites in the subject field, and then down in the note field', so we must adapt it in relation to what the caseworker needs to record, what it looks like from the data subject's point of view, what the context of the meeting is. Is it someone working with building permits or forced removal of children? Those are two different things. If your name appears in one context as opposed to the other, it has wildly different meanings" (Information security coordinator, December 2018)

Implementation of GDPR rules for calendar invites was unpredicted, but urgent. Microsoft Outlook was used multilaterally as Fairview's dedicated e-mail and calendar client, but as proprietary software, it did not meet the minimum technical requirements for encryption prescribed by Fairview's cybersecurity policies. Besides being vulnerable to hacking, the invites were often used by case workers to comment on the nature and purpose of a given meeting, when scheduling it, and while this was not controversial for domains involving little personal data, it was problematic for social services dealing with sensitive issues. To conceive a meaningful data governance arrangement that could encompass the entire organization with its multiple practices for recording different data

in the calendar invites, the Information security coordinator knew it would require similar negotiated resolutions to conciliate competing concerns between domain specific work practices, organization-wide coordination and the data protection regulation. The coordinator acknowledged that devising effective data governance could not hinge on individual practitioners translating new, general rules to their own situation:

> " (…) this thing where you expect people to be able to translate or derive meaning from a legal document into guidance by themselves, we can't demand that from people who have a completely different background and focus. It would be like if I was given a manual for my car, and then I could just fix it myself when the turn signal wasn't working "(Information security coordinator December 2018)

In working with contextual implementation of GDPR, the Information security coordinator formed early experiences with a new form of action arena, the data venture, which enabled new actions and outcomes. Although essential exploration occurred, it was not until the end of the episode, where competing concerns between data governance in a technical department and a citizen's complaint about data protection had been resolved through a data venture that making use of the new action arena showed actual results (described in next subsection 5.3.3).

5.3.3. ZOOMING OUT

The beginning of this episode coincided with the official deadline for instatement of GDPR in May 2018. At the same time, media coverage of the regulation in major national news outlets were largely dominated by two different perspectives. On one hand, newspapers emphasized the extreme costs incurred by organizations in preparing for and implementing the directives in GDPR (Kjær 2018a; Munkholm 2018), and reported success stories about companies that had managed to convert the involuntary investments in data governance into meaningful business value (Blædel 2018; Hvas 2018). On the other hand, newspapers also announced that while citizens had now reclaimed some control over their data with this regulation (Littauer 2018; Scheuer-Hansen and Guldagger 2018), public data protection agencies lacked resources and would be hard-pressed to oversee compliance in any meaningful way (Jarlner 2018; Kjær 2018b, 2018c).

Citizens in turn became extremely vigilant about how their data was treated. This was also reflected in the annual report from the Data Protection Agency for 2018, which showed 8756 new cases were created after May 25. Of these, 2249 cases (roughly 25%) related to guidance and counseling in response to specific inquiries (Data Protection Agency 2018, p. 16). Even though 1376 formal complaints were filed after May 25, of which 1005 (roughly 73%) were against private companies, the agency conducted only 225 audits, of which 135 were in public organizations, 61 were based on citizen requests, 12 were in private companies, 11 were based on issues covered in media and 6 were general audits (Data Protection Agency 2018, p. 18).

A seemingly disproportionate attention to public authorities' treatment of citizen data also affected Fairview, when a citizen filed an official complaint against the municipality in June 2018. Through a web search on their own name, the citizen had discovered a freely accessible hearing for an old building permit application, which listed their full name, address, phone number and e-mail. Since the case had long been completed, the citizen directly instructed the municipality to delete the data multiple times during May 2018, but after receiving no response, decided to file a formal complaint with the Data Protection Agency. Fairview ultimately rejected the request to delete the data with reference to legal requirements for public authorities to maintain such records, but while the Data Protection Agency ruled in their favor, they also urged the municipality to reconsider how personal data was administered in open access to building permits.

Handling building permit cases was supported by a set of complex, but streamlined processes, and relied on multiple internal and external documents, in addition to public hearings and the department for Technical and Environmental Services therefore initially dismissed to amend the treatment of personal data. Even though this practice was legally sanctioned by the agency, it still received close scrutiny both from additional citizens, Fairview's own DPO and the department for IT/Digitalization, who wanted it amended. Yet, producing a second version of all these documents without certain data for the public archive would require substantial additional effort, both to develop and maintain. Before the formal complaint was concluded in November 2018, Technical and Environmental Services grew dissatisfied with the surrounding pressure and decided on a compromise.

Instead of producing duplicate documents, they envisioned the design of a machine learning tool, which would redact personal data in the documents, if they were viewed through the public archives, but leave the originals unedited and accessible to case workers inside the municipality. To begin with, a developer from IT and Digitalization was tasked with specifying requirements, but local practitioners in Technical and Environmental Services had better contextual understanding of what the solution was supposed to address and therefore assumed responsibility for the venture. By the end of November, the department had developed and implemented a simple, cheap PDF redaction solution, which they supported themselves. Citizens used their NemID to access the same archive as before, and when opening a case, they were met with a loading screen informing them the document was being 'cleansed' and in the final view, any personal data were redacted.

Essentially, the PDF cleansing tool constituted the material outcome of a dedicated data venture, which had emerged to resolve the competing concerns between interests of citizens, public authorities and multiple local practitioners. Modifying existing data governance arrangements was initially resisted by Technical and Environmental Services because duplicating documents did not resonate with the local conditions for how practitioners in their department were conducting their work, even if it formally solved the problem. As Technical and Environmental Services learned they were better

equipped to specify and manage development of the solution, the IT department accommodated and withdrew. After the solution had been implemented, other departments in Fairview dealing with open access to public records contacted Technical and Environmental Services looking to adopt their solution.

While resolution of these competing concerns were not expressly addressed as a data venture in Fairview, the Information security coordinator later referred back to this series of spontaneous, unfolding events as valuable learning experiences. Managing problem-solving across formally established domains, hierarchies and organizational boundaries offered early insights into how data ventures as emergent action arenas were effective in enmeshing managerial, operational, social and material activities for devising data governance. When a problem emerged, the corresponding organizing was not immediately fixed in existing structures or formalized, but rather allowed to co-evolve with and address concerns as they became salient. Focal actors, such as the practitioners in Technical and Environmental Services were afforded enough autonomy to negotiate a sustainable resolution working for them, which also meant that the citizen(s) received a compromise, even though their original claim was rejected. Roles and responsibilities were not formal or enforced but also negotiated and adapted to fit the situation; even though the IT department usually coordinated cross-cutting collaborations for IT acquisition, they did not enforce this role, when it did not make sense.

5.3.4. EPISODE SUMMARY

The second episode *Experimenting with strategies for devising data governance* immediately followed episode #1, when the dust from the frantic GDPR implementation had started to settle. Like most organizations, Fairview had expected auditors to arrive on the date in May 2018 to inspect compliance but discovered this was not the case. Instead, newly formed concerns for data as a collective, organizational resource challenged preexisting arrangements, structures and hierarchies within the boundaries of Fairview municipality. New data-centered initiatives, both directly and indirectly shaped by requirements from GDPR were not immediately compatible with status quo in Fairview and significant resistance emerged. Externally defined and imposed rules were opposed and perceived either to be too restrictive, too abstract or too ambiguous for practitioners to adhere to them. In response, the Digitalization director and a newly appointed Information security coordinator switched back and forth between action arenas to leverage different options for resolving general and specific issues.

What signaled the conclusion of this episode was an elusive, but important shift in how data governance was perceived and accomplished in Fairview. Extensive work involved in mapping IT systems, understanding where data was located and who was allowed to process it for which purposes, was no longer considered an isolated, temporary incentives for remaining compliant with GDPR. Rather, it was the foundation for evolving data governance arrangements which would make sense for Fairview as organization in practice. GDPR had been an effective driver in pushing concerns for data as a collective

resource to the forefront, but the imperatives for data protection had been absolved into a more general understanding of data governance and by the end of episode #2, the Digitalization director looked at GDPR as a hook for pursuing other data-centric initiatives.

To ensure compliance with the new rules following from GDPR, the IT manager, the Digitalization director, and the Information security coordinator had enacted polycentric governance through elaborate monitoring and sanctioning practices, even though fear, confusion and anxiety had been major forces in shaping these practices. While GDPR promoted stronger incentives for adopting coordinated strategies for governing data as a collective resource, these incentives were still not considered intrinsic to practitioners in Fairview. This changed throughout the episode, as the Information security coordinator experimented with different strategies for shaping, forming and adapting rules in collaboration with practitioners. Early experiences with data ventures as an action arena demonstrated that strategies for devising data governance arrangements were more effective, when they actively included practitioners and allowed them to negotiate rules that corresponded with their own local context.

5.3.4.1 Highlights from Episode #2:

- Focal actors were primarily the Digitalization director and a newly appointed information security coordinator.
- Instatement of GDPR led to increased relative importance of data from the outside and resulted in massive exogenous pressure on practitioners within Fairview to accept newly imposed boundaries and adapt carefully crafted operational rules.
- The Digitalization director evolved activities in mapping IT systems from being solely a technical task, to sketching boundaries and worked to ensure they were continuously enacted by groups of individuals with mutual responsibilities.
- The Information security coordinator became an official monitor and succeeded in gaining the trust of other practitioners to report violations, which provided her with information about key issues and allowed her to sanction rule infractions.
- Experimentation resulted in the discovery of a new action arena, the data venture, where problem-solving could unfold emergently and responsively among otherwise heterogenous practitioners.
- A specific data venture was brought into being, where practitioners engaged in multiple interweaving, managerial, operational, social and material activities to devise specific operational rules for data use.

5.4. EPISODE #3: ACTIVATING COLLECTIVE PARTICIPATION

JANUARY 2019-MARCH 2019

By January 2019, tensions between the competing concerns for how to treat data in domain specific work practices and in the data protection regulation grew increasingly salient. Although the need for devising data governance arrangements for calendar invites had emerged in the previous episode, the information security coordinator had tried to come up with some normative general principles, without result. While accomplishing significant results, the majority of the Information security coordinator's efforts were concentrated outside formal hierarchies and mobilizing collective participation ended up constituting most of her work:

> "Most of the regulation says 'all employees must', but how do you actually vouch for this? Everyone should be informed about the rules, but can system owners take responsibility for their employees' knowledge of data protection? Here is the dilemma between whether to train your employees to understand the rules for individual systems or focus on creating general awareness in the entire organization" (Information security coordinator, February 2019)

Previous efforts by the Digitalization director and the Information security coordinator had been focused on developing formal documentation, data processing agreements, and system overviews in a somewhat detached fashion, since this was in preparation for GDPR. While most of this work continued in episode 3, it progressively grew to encompass multiple other initiatives in Fairview. Tensions emerged between concerns for new data governance arrangements not pertaining to GDPR and established norms and routines within certain individual municipal professions. As one example, these tensions manifested two data ventures, which evolved throughout the episode.

At the outset of episode 3, devising data governance arrangements had progressed from defining IT architectural principles and implementing Information security policies towards negotiating local resolutions and rules for how to treat data. Several issues proceeded as the two focal actors of the episode, the Information security coordinator and the Digitalization director, worked to mobilize collective participation. These issues indicated that establishing new data governance arrangements was difficult because it required co-evolving data practices with profession-specific work practices and revisiting normative concerns for data. Polycentric governance was enacted by readjusting boundaries of data as a collective resource, facilitating collective choice through data ventures and improving congruence between arrangements and practices through situated resolutions.

5.4.1. COLLECTIVE ACTION THREATS

While polycentric governance enacted in relation to GDPR sufficiently curtailed threats posed by weak incentives for adopting coordinated strategies to data as a collective resource, the renewed attention to data governance as an organizational endeavor in turn exacerbated previous tensions caused by high degrees of heterogeneity across different municipal domains. As incentives had moved beyond compliance with exogenous rules, the internal pressure to adopt normative concerns for data and accept consequent readjustments to deeply rooted work practices characterized threats to collective action during this episode.

5.4.1.1 Tensions between collective concerns for data and localized work practices

Since most data governance in Fairview prior to GDPR was determined by large domain-oriented IT systems, the concern for data as a resource was deeply embedded in individual, departmental work practices. Little attention was paid to data separate from these IT systems and work practices, which made it difficult for the Information security coordinator to conceive organization-wide principles for documenting how user access rights had been granted:

> "User access control must contain certain things that I try to develop a general instruction for (…) Each system owner has access to decide for specific data sets, and IT is responsible for setting password requirements that are followed by everyone. Do they have legal authority for processing data, or do they have to obtain consent? It is unclear to everyone. The Data Protection Agency does not have enough professional insight into the systems and municipal domains, so it is generally difficult to get a response from them." (Information security coordinator, February 2019)

According to GDPR, access and processing of data must be under purview of one of six lawful bases[13]. For a municipal IT system in a given domain, the right to process data may be sanctioned by Danish legislation as part of their public function, but if not, consent must be collected from the citizen. Yet, it was unclear, even for the Data Protection Agency, how to determine the rightful base for municipal IT systems, because their data processing was so closely entangled with their professions, which the agency had insufficient knowledge about. Essentially, no one system owner, function or public

[13]With consent from the individual, as necessary by a contract with the individual, as part of a legal obligation specified by law, to perform interests vital for the individual, as part of a public function or task sanctioned by regulation, and as part of a legitimate interest within the organization

authority had a complete understanding of all elements; data sets, user access in the IT systems, relevant legislation and data protection directives.

While certain measures could be taken with technical restrictions to ensure compliant treatment of data, most of the necessary changes would involve changes in behavior.

> "It is the question of IT systems versus business processes; mapping the systems does not necessarily mean having an overview. It's about pushing some chairs closer together, with some people who may not have wanted to take responsibility for specific data in the past, but they have to now. Awareness is absolutely central to capturing the small, informal things " (IT manager, February 2019)

According to the IT manager, there were only so much the IT and Digitalization department could do in defining official principles. Most of the issues would not necessarily be visible to them, so the local system owners would be pivotal in understanding data governance rules and changing the necessary behavior. As a result, it took time to discover 'the good questions':

> "GDPR is deeply entangled with workflows (…) A routine change is quickly formalized in Technological and Environment Services, but their way of handling data is like facts. In social services, they instead have a holistic overview, and try to be proactive, where Technological and Environment Services acts on individual cases and is more reactive. In one case concerning a request for public access to documents, an employee had to tick off documents for release. A response from a hearing was in the system and there was a spreadsheet with social security numbers from the neighbors. A list of 100 numbers was released from the department. For a new release process, they went in and changed a routine to prevent it from happening again. But asking the good questions takes time to figure out, because they already had a very formal procedure in advance" (Information security coordinator, February 2019)

The Information security coordinator had little opportunity to predict and prevent such issues, since her insight into the work process for the Technical and Environmental Services domain was limited. Additionally, they had not themselves predicted this problem, even if they were quick to formalize the necessary adjustments in their IT system. Forthcoming initiatives in the Information security coordinator's pipeline were also characterized by similar issues:

> "Records management is a huge to-do on my list. It crosses over with multiple difficult topics such as routines, data quality, core responsibilities, system owners, our electronic case management system. System owners on all the different systems manage records in all sorts of different ways related to their work routines, local needs and ways of doing things. For system

> owners, records management is also influenced by the GDPR angle, with different quality requirements, but the course in records management is just general." (Information security coordinator, February 2019)

For Fairview, records management was mandated by law, but how legislation on this for the different municipal responsibilities intersected with new rules for data processing in GDPR was unclear and the Information security coordinator had little idea about how to even review or document compliance in this regard. In addition, since these practices for treating data were deeply embedded in local work practices, it also made it difficult to determine how data sharing occurred within Fairview's organizational boundaries:

> "For sharing data across functions, both formally and informally, our focus on it, I wish I had a definite answer, but I actually think we have a point to pay attention to. There is something we need to work on" (IT director, February 2019)

Consequently, existing operational rules for data use in Fairview were so ingrained in how work was performed that they were largely invisible to the Information security coordinator, who was tasked with devising new arrangements. In certain areas, data practices would only resurface, if a violation occurred and it was difficult to know in advance where and when this would happen. The entanglement between data and work practices posed a substantial threat to collective participation in new governance arrangements, since a lack of insight made it difficult for the Information security coordinator to devise meaningful rules.

5.4.1.1 Resistance to normative approaches to data

Instatement of GDPR involved several well-defined data types, such as personal and sensitive data, which had somewhat clear requirements for processing. Although Fairview had gained experience with developing data governance arrangements not directly pertaining to GDPR compliance, such as the PDF cleansing tool, citizens and practitioners were still confused about how the normative concerns from the regulation related to them:

> "There is a bit of confusion about the different types of personal data, such as the ordinary and the sensitive, and then I think something is missing … it all gets mixed up, so we get complaints that you can see other recipients' email addresses, on an e-mail invitation to a Christmas event at a nursing home, and then there is a relative who complains that her email address can be seen by all the other recipients who are also relatives of residents of this nursing home (…) there is a lot of confusion regarding these categories and it is also internal" (Information security coordinator, February, 2019)

While the incident was not directly related to personal data protection rights, the data was personally identifiable, which meant it might have been covered in a different

context. Since concerns for data as a collective resource had been largely absent before GDPR, the normative concerns implied in the regulation filled a vacuum in other contexts, where it was not necessarily applicable.

As these normative concerns for data were embedded in data governance arrangements supporting GDPR, certain initiatives were also met with resistance from those not sharing the same concerns. When the Information security coordinator announced to the IT and Digitalization department that Fairview would be audited on every single IT system and therefore had to procure documentation on data processing agreements, auditing statements and procedures for managing data access rights, it was met with resistance. The IT developers knew that user access was not completely formalized with some 200 users unaccounted for and questioned who would be qualified to assess how this was handled in their IT systems:

IT developer: "Do we really need to know all this right now? Can't we just say we forgot it? Who is overseeing this and how do you know they are knowledgeable?"

Inf. Sec. Coord.: "Right now it's about formal documentation on what we've been considering on the topic. We need to show that we know our IT systems. It is not an IT inspection, so we do not have to look at the systems, but instead show that we are compliant with the regulation"

(Team meeting, IT and Digitalization, February 2019)

The IT developer appeared to understand the audits as a process involving someone looking 'into' the different IT systems to account for all users and their different data access rights, but it was not this type of data governance arrangement implied by the Information security coordinator. Rather, it was about devising a procedure for assessing who had access to data sets and how these rights were designated and managed in IT systems.

In addition, resistance against normative concerns for data made it difficult to devise organization-wide data governance arrangements, for several reasons:

> "We can't call it policies, even though it would normally be called that. Guidelines don't work either because it doesn't specify the 'how', but an instruction is okay (…) We wanted to publish [a new instruction] on the employee intranet, but it was sent out individually to everyone. The instruction was 100% behavior-based, as opposed to technical implementations, but very general (…) We define something in general, which is either loosened or tightened, when we receive feedback from the organization and an entire undergrowth of bad habits emerges" (Information security coordinator, February 2019)

While most of the data governance arrangements devised by the Information security coordinator essentially constituted policies or principles, they could not be defined as such. Moreover, as general instructions were distributed throughout the organization, the subsequent responses from individual practitioners to the normative ideas about data in turn revealed multiple issues in current practice, which were previously unknowable and impossible to pinpoint. Confusion about how and when normative concerns for data as a resource would apply in specific, local contexts therefore posed a significant threat to mobilizing collective participation, specifically for arrangements which would be perceived as normative

5.4.2. ENACTING POLYCENTRIC GOVERNANCE

From past episodes, polycentric organizing in Fairview had evolved significantly from defining the early boundaries for a common data resource system in Fairview to resolving second-order problems to secure support, arranging elaborate monitoring and sanctioning practices and improvising data ventures as a new action arena. Yet, the Information security coordinator had previously attempted to mobilize collective participation through general initiatives, with little success. Recent experiences with data ventures as action arenas had however demonstrated the benefits of negotiating local resolutions for general arrangements with practitioners in their contexts to ensure their participation.

During episode #3, polycentric governance was therefore primarily enacted through data ventures, which emerged in response to specific competing concerns between general rules and local practices. At the same time, much attention was paid to the idea that activities within each local government domain could be boiled down and conceptualized in a single fundamental task, for example "to create learning" for the school area. Yet, for the IT manager, this was an oversimplification:

> "Respect, ethics and fear take up a lot of space, especially in cross-cutting processes, such as emails. But this idea of 'the fundamental task' is in fact an abstraction, because it is many small tasks that together make up a big one and end up as a result"(IT manager, February 2019)

While domain-oriented IT systems supported some fundamental tasks within professional domains, devising data governance arrangements would also have to take into account the many small-scale, informal processes, such as e-mail, occurring in local practice. In response, a data venture unfolded to address specific concerns related to data sharing in the calendar-function of Microsoft Outlook. Polycentric governance was enacted by readjusting boundaries for how to treat these data in the common resource system, which were outside formal, domain-determined governance arrangements. Readjusting these boundaries enabled the Information security coordinator to define data sharing and access rights for contextual situations, which improved congruence between the new rules and local practices. Polycentric governance was also enacted by refining

new data governance arrangements for data sharing in response to collective input from different practitioners.

The Information security coordinator and Digitalization director were focal actors, both in establishing and managing data ventures, but also in devising consequent data governance arrangements. Although the concerns in question had evolved as a response to implementation of the GDPR, polycentric governance in this episode was much less about developing formal procedures and documentation and much more about devising arrangements which were sustainable and feasible both on local and organization-wide scale.

5.4.2.1 Readjusting boundaries for data as a collective resource

In preparing for instatement of GDPR, Fairview had reviewed processing of personal data in most of their IT systems, which were developed within municipal domains. The regulation specified a series of technical measures for processing personal data and besides encryption, these measures involved rigorous requirements for localizing and deleting all data about a citizen upon request and for limiting processing and access to data for unauthorized users *within* organizational boundaries. In Fairview, Microsoft Outlook was used multilaterally as the organization's dedicated e-mail and calendar client and entangled in a wealth of formal and informal rules for data use. While originally a practical tool for internal and some external coordination, it had grown to constitute a central, unofficial IT system in most work practices, making it difficult to oversee compliance.

Since Outlook did not comply with IT security policies in Fairview but was still used multilaterally for a variety of known and unknown tasks, any data governance arrangements would have to address behavioral changes. When the Information security coordinator began to tackle use of the calendar-function in January 2019, and specifically data sharing in calendar invites, multiple, competing concerns materialized. First, Fairview had an open calendar policy, which meant details on subject, time and place for appointments had to be visible to all practitioners to better facilitate coordination and planning. Outlook was also used to coordinate with external parties, such as citizens or contractors, such that the content of any such invites would also be visible to the rest of the organization.

Second, when Outlook was used to schedule and coordinate meetings within the organization, it could simultaneously be used for booking conference rooms. Each conference room was assigned a unique e-mail address, and if added as an invitee, automatically booked for the duration of the meeting. Each conference room was then equipped with a little screen outside (see Figure 6), showing whatever had been noted in the 'subject' field of the invite, all accepting participants as well as who had created the invite. In Fairview, the administrative departments making out city hall were housed in a newly constructed, multifacility building named "Fairview Commons", alongside citizen

services, a local branch of the regional police, a restaurant and a multifunctional gymnasium. While conference rooms were accordingly located in different zones; designated as open to the public; accessible only to administrative personnel and; restricted to individual departmental employees, the placement of these screens and other info boards made data in invites broadly visible to others.

Figure 6. Sketch of meeting screen from Fairview

Under the purview of GDPR, a calendar invite for a meeting titled "Meeting about removal of child" between caseworkers from the Children and Youth department and parents identified by their full name and address constituted sensitive data and therefore needed to be governed accordingly. Firstly, an invite containing such data would be compromised by Fairview's open calendar policy, where all other employees could essentially view the appointment in a caseworker's calendar. Secondly, if the meeting was booked within a conference room, even in a restricted zone only accessible by other caseworkers, all access to sensitive data still needed to be logged, so Fairview could at all times document that only authorized employees had processed these data in accordance with the rightful legal base as specified by GDPR. For the Information security coordinator, devising rules for how and when to share personal data in calendar invites therefore became urgent.

When she began to address the issue, she immediately had to confront another related organization-wide practice in Fairview. When practitioners attended meetings outside Fairview Commons in relation to their municipal functions, they were entitled to certain financial reimbursement relative to the total number of kilometers of their trip. The calendar function in Outlook had previously functioned as a local mechanism for checking whether reimbursement requests were consistent with calendar activity. A common practice at the time was therefore to meticulously specify address, full name of

citizens and the professional purpose for having the meeting, even when the topics were highly personal and sensitive, because it was considered a prerequisite for getting travel expenses refunded:

> "This is a problem specifically across Fairview municipality; being able to check driving in the work calendar was a local provision once and not a formal requirement from the Ministry of Finance. Reporting in the system for travel allowance requires only that you can refer to an address and what you were there to do. And then the question arises; what is the need for writing addresses in calendar invites then? Formerly, it was to satisfy local requirements for control and reimbursement, but now it is unclear" (Information security coordinator, February 2019)

Although applications for travel reimbursement in the dedicated IT system, only required practitioners to document travel distance, address and purpose, some were still convinced aligning this with calendar activity was a necessary, formal requirement set by a central ministry.

Even after GDPR was instated in 2018, where sharing of sensitive data in this manner was widely prohibited, practitioners in Fairview had not changed their behavior. Before January 2019, the issues were addressed by marking sensitive appointments as "private" in the calendar invite, preventing the data from showing up on meeting screens and in open calendar views. Yet, since Outlook did not meet technical requirements for encryption and storage of sensitive data, this practice was still compromising. Another central directive specified by GDPR was the right for any data subject to know exactly how organizations were processing which data about them and why. If practitioners were illicitly recording and sharing data outside secure, formally governed IT systems such as through calendar invites and e-mails, it would either be vastly time-consuming or downright impossible to produce accurate documentation for how data was processed upon request.

In response, a dedicated data venture began to unfold, as the Information security coordinator had to negotiate multiple competing concerns in order to devise sustainable data governance arrangements for the calendar function in Outlook:

> "… calendar entries as opposed to documentation requirements; Outlook is not secure enough in relation to where personal data may be stored, and it is difficult to find all data if the citizen seeks access to documents, but 'Where should we meet' is critical for a meeting, even if it can also be quite personal. How do we decide then? (…) We are trying to find a common ground between 'this is too rigid' and 'this is too open for interpretation' and 'we must note this because otherwise we will not get money'" (Information security coordinator, February 2019)

Even though Outlook was previously considered a coordination tool, normative concerns for how to govern sensitive data as a collective resource now meant no clear boundaries could be upheld between the practicalities of scheduling meetings and the formal requirements for documenting data access. In order to appropriately define access rights and devise rules, the boundaries needed to be readjusted. As a result, the coordinator instead drafted a new "meeting typology" for Fairview, which differentiated between three types: special, confidential meetings; general, personal meetings and non-confidential meetings. Since Outlook was used multilaterally, it was more feasible to devise rules according to the nature of the meeting itself, rather than for where and in which department the meeting occurred:

> "For example, can't meetings in Technical and Environmental Services also be sensitive? It's hard to slice the rules by departments, so it became by types instead. The examples are local and customized, for example different types of meetings with different examples for which data are okay to share" (Information security coordinator, February 2019)

The different meeting types were conceptualized in an organization-wide guideline, which specified how each meeting type was defined, which data could then be shared where and with whom, including practical examples for how this would look. The guideline also worked from key assumptions about data minimization and context consideration:

> "The context surrounding the calendar entry determines how sensitive it is and thus how important it is to obscure the identity of the citizen or employee. This means that you have to ask yourself if outsiders will be able to recognize specific people from data in your meeting invite and whether it will be acceptable for that context. Even if only the name, address or telephone number is written, for example, this data in combination with other data may reveal sensitive or confidential circumstances about the person in question. (…) It depends on what the calendar entry is about, and which employee is responsible for it." (Guideline for handling personal information in Outlook calendar entries, Fairview municipality, January 2019)

By readjusting the boundaries for how to treat sensitive data as a collective resource within Fairview, the Information security coordinator managed to negotiate a resolution between multiple competing concerns for data sharing in calendar entries, again involving both social and material activities. In turn allowing, it allowed the coordinator to devise more sustainable arrangements for access to these data.

5.4.2.2 Facilitating collective choice to improve congruence

While the new guideline was conceived with a keen eye for the specific challenges facing Fairview, such as the open calendar policy, the physical meeting screens and the complicated reimbursement process, it had not been negotiated directly with

practitioners in their local working environments. Even though the guideline focused on actionable instructions as opposed to abstract policy language and even afforded individual practitioners enough autonomy to determine from contextual considerations which meeting type to work from, the organizational response also indicated that collective participation and engagement with the new rules had not been facilitated with practitioners.

Initially, the Information security coordinator considered approval of the guideline from the Information Security Committee essential in gaining this engagement from the rest of the organization. The committee was made up of the executive management group, and consisted of the city manager, two executive directors, four group managing directors from each of the professional secretariats for Children and Youth, Elder and Disability, Employment and Health, Technical and Environmental Services, two group managing directors from the administrative departments of Culture, Citizen and Planning and Executive City Council Management, as well as the Chief Financial Officer (CFO) and the head of HR. According to the Information security coordinator, their official stamp of approval would not only be an endorsement, but also add more weight to the new rules and preemptively avoid infractions:

> "I am writing the draft, and then in the first place, it goes to [the IT manager] and [the Digitalization director], probably only [him], and then, because we have decided it is so important, because it concerns so many in the organization, it goes to executive management, for them to nod to it, and then it also has … yes, another thing is that it then has a slightly greater impact, more weight because yes, the top management has said 'this is what we have decided that our level of security is'" (Information security coordinator, January 2019)

While the guideline was easily sanctioned by executive management, the responses from the rest of the organization still indicated difficulties in translating it operational rules in local practices. After the guideline was published in Fairview, the head of the Substance Abuse Rehabilitation Center contacted the Information security coordinator, because they wanted their department to become more GDPR compliant:

> "They developed a presentation for their own department but would like feedback on the content. (…) they have very specific questions about phone numbers, text messages, calendar entries after the new guideline, because now they are in doubt. What applies? The department head personally cares about this matter, there is no resistance, no one says it's not important, and everyone agrees it's a good idea. So now they want to know how to balance what is right with what is practically possible. The manager has asked for it, not because her employees resist, but because they're close to vulnerable citizens, their work is sensitive and thinking about this is a natural part of their job" (Information security coordinator, February 2019)

The request from the head of the Substance Abuse Rehabilitation Center again reflected the need for brokering local accommodations to organization-wide rules, even if these rules were already practical, specific and sanctioned by top management levels in Fairview.

The normative concerns for governing sensitive data as a collective resource, which were embedded in the new guideline, did not meet resistance from employees working with substance abuse, because concerns for privacy and protecting sensitive information about vulnerable citizens were already ingrained in their job. Their interests in adapting these rules were not motivated by fear of harsh sanctions, but rather by voluntary compliance because their own professional values seemed to resonate with the underlying norms of the guideline. These trends were also reflected in questions from other social services departments, where practitioners had been used to thinking about protecting sensitive information:

> "I get questions from Children and Youth and Elder and Disability, and Employment [on the guideline]. In the case of the Elder area, they have always been very aware of the really sensitive information they work with, so they have a code of patient confidentiality, and that is very much in line with the regulation" (Information security coordinator, February 2019)

Facilitating an opportunity for practitioners to voice their doubts and uncertainties was vital in mobilizing their collective participation in the organization-wide arrangements, even when the rules were already perceived as meaningful and valuable within the individual municipal professions. Despite her best efforts to make the general guidelines as practical as possible, by the end of this episode, the Information security coordinator acknowledged that improving congruence between general rules and local conditions would have to involve actively brokering situated resolutions with practitioners:

> "Information security is a way of thinking, where one has to stop doing something, often for the sake of the citizen. It is difficult to convey awareness (…). Most people ask for help themselves, because they want to coordinate their efforts. (…) The language is governed by 'get data under control', but inevitably everyone must translate this themselves and it opens up for new ramifications of the subject. You relate to something very abstract, but it only shows up when it meets practice. So, it must be used in practice and it takes a long time before you get it under the skin." (Information security coordinator, March 2019)

Rather than considering the organizational response as problematic or even preventable, the Information security coordinator recognized the process as necessary for developing awareness and anchoring data governance arrangements in practice. While organization-wide rules had to be conceived in a general manner to cover the breadth of functions, it would not be viable for the coordinator to attempt to predict the ramifications for individual domains, because they would not truly unfold before meeting local practices.

By the end of the episode in March 2019, the Information security coordinator had received multiple queries and consequently drafted a set of supplemental instructions for the guideline. The instructions focused on special, sensitive meetings, where the sharing of personal data in specific contexts rendered them sensitive and therefore subject to different governance arrangements than if the same personal data were shared in normal or non-confidential meetings. Unlike the guideline, the instructions zoomed in on specific workflows, where doubts about data sharing could arise. For example, including address data on citizens could only be justified under very specific circumstances:

> "Addresses may only be entered in the note field of calendar entries, and only if there is a real need for it. Legitimate needs may be for planning or ensuring the safety of municipal employees:
>
> - For managing a full day of external activity
> - For colleagues to be able to cancel or take over appointments
> - For colleagues to know where an employee is, if the appointment may involve potential risk to the employee"
>
> (Supplemental instructions to Guideline for Outlook calendar, Fairview municipality, March 2019)

The specific circumstances had spurred directly from the Information security coordinator's interactions with different practitioners, when they sought her advice and also included screenshots of examples from Outlook; examples which the coordinator did not anticipate, when conceiving the original guideline. By facilitating collective choice for how the rules should be translated and put into practice, the Information security coordinator were able to devise arrangements more congruent with the local conditions they were meant to address.

Publication of these supplemental instructions simultaneously signaled the resolution of a data venture which had evolved to enable the Information security coordinator to devise rules for data sharing in calendar invites, which were both multilateral, bounded and actionable enough to remain sustainable in several local practices. The outcome of the data venture resulted in Fairview's first organization-wide data governance arrangement, which had gradually evolved in response to multiple competing concerns, which were negotiated and accommodated, as they became salient. Moreover, as the Information security coordinator constructively leveraged feedback and organizational responses from practitioners in shaping and interpreting rules, she managed to activate collective participation in organization-wide data governance arrangements, which were congruent with local conditions.

5.4.3. ZOOMING IN

By the end of episode #3, the Information security coordinator and the Digitalization director, who remained focal actors in advancing previous data ventures, had gained valuable experiences with engaging collective-choice arenas for resolving competing

concerns, but only *within* Fairview's organizational boundaries. The third episode had seen resolution of a data venture, which brokered a substantial, multilateral arrangement across departments, subject domains, hierarchical levels and decision-making structures to govern certain data as collective resources within Fairview. While the end of episode #2 did see resolution of a data venture which evolved in response to external pressures from citizens, the resulting data governance arrangements eventually only involved operational rules for a single, internal department in Fairview (see section 5.3.3). Leveraging these experiences, the Information security coordinator and the Digitalization director began to confront emerging tensions in a third data venture, which involved competing concerns for how to ensure appropriate data sharing between family care consultants and foster parents.

When a child was brought into care with a family, it was custom for the dedicated family care consultant in Fairview to create an action plan for the child in close collaboration with the foster parents and other relevant staff, if needed. The action plan was conceived in a standard Microsoft Word template and functioned as a portfolio, where foster parents would provide frequent updates directly within the document and return it to the family care consultant, who would record progress in a corresponding IT system and address any issues raised by the parents. Previously, this occurred simply by emailing the action plan directly to foster parents, who would store it on their personal computer, fill out relevant fields and return it by email again to the family care consultant. Following publication of the Outlook calendar guideline in January 2019, head of the family care department had become aware that this exchange form was highly inappropriate. Any data pertaining to foster children and their assigned care families were both sensitive and personal. Outlook did not live up to encryption and security standards in the first place, but the fact that foster parents were storing and processing highly sensitive data on their own personal computers were critical violations of GDPR. The department head therefore contacted the Information security coordinator and the Digitalization director, looking to develop an alternative solution.

Family care consultants in Fairview knew from other municipalities that this problem had been resolved by providing each set of foster parents with a dedicated laptop living up to the necessary IT security requirements. Yet, most of the social workers and family care consultants also felt this was not an optimal solution, since the digital literacy between foster parents varied significantly:

> "The IT landscape is very varied. There are many interests (…) It also requires insight into the domain IT system and the ESDH[14] for journaling requirements. We want to focus on roles rather than individuals, so that one

[14] Electronic document and records management system

> of us can take over in case of illness. But what can we do for the foster family as citizens?" (Social worker, February 2019)

In rethinking how these action plans could be securely exchanged, without burdening foster families with new technologies, other concerns began to emerge. A potential new solution would not only need to take into account the many requirements for how data was collected through action plans for journaling requirements and records management. If emailing was removed altogether, the social worker also wanted the new solution to enable secure, legal data sharing between consultants.

Initially, a developer from the IT and Digitalization department suggested recycling an existing solution already used by foster parents for registering transportation expenses incurred in relation to the foster child. In the web-based solution EmployeeOnline, foster parents recorded various data directly into an online form, which could then either be saved for later completion or submitted to the family care department for processing. While the solution was easy to use, adhered to encryption standards and used the mandated NemID as log in, it was also meant for very simple data processing. Another recycled resolution involved creating a dedicated mailbox in e-Boks, where foster parents could securely exchange communications with family care consultants, but, it would quickly become convoluted for users in practice, requiring manual selection from a drop-down menu of multiple mailboxes, logging in with two-factor authentication for writing a single message and no template for filling out information.

By February 2019, the data venture had grown to involve two social workers, a foster care consultant, a pedagogical and psychological consultant, the Digitalization director, an IT developer and the Information security coordinator. One potential resolution involved a behavior-based arrangement, where new and existing foster families needed to learn about GDPR, similar to what all employees in Fairview underwent before the regulation entered into force in May 2018. Yet, all material on information security was directed at municipal practitioners, not citizens:

> "There is a general demand from several departments for material which can be sent out, but [what we have] was originally written for employees in the municipality, and the foster families are citizens. There are many areas with special rules that make it context specific. We can consider mandatory GDPR training of foster families before they arrive" (Digitalization director, February 2019)

Although GDPR training would not involve developing new technological solutions, it would still require developing a citizen-directed contextualized approach to GDPR from scratch. Eventually, both social workers and family care consultants agreed that any solution would need to offer additional value besides just meeting basic requirements for documentation and information security, both to foster parents as citizens and employees in Fairview:

> "We must either inform [foster parents] about how to do [GDPR compliant data sharing] or develop a technical solution that ensures the communication complies with requirements from the beginning. I think we should see this as an opportunity for changing communication practices between foster families and consultants (…) Again, thinking of the potential use cases rather than what foster families are likely to do wrong. We are looking for the least intervention in their everyday life, the cheapest solution for us to maintain" (Social worker, February 2019)

Tensions initially proceeded from an inappropriate data sharing practice, but multiple other concerns had gradually materialized. By the end of episode #3, a prospective data governance arrangement needed to function across organizational boundaries but satisfy formal documentation requirements; it needed to provide new communication practices but still constitute least possible intervention in existing practices and; it needed to ideally involve developing a new, but cheap technical solution. As the Digitalization director and the Information security coordinator had previously leveraged collective choice in negotiating resolutions that were both sustainable and congruent with specific local conditions, a preliminary outcome was situating the data venture in the foster care context:

> "User involvement of foster families [is necessary] to find the good process. Does it work? (…) What does it look like in a foster family context? The department of family care will take the lead on developing, the department for IT and Digitization will provide input and quality assurance [about] communication and storage of sensitive, personal data. The foster families will probably also need to have an information security introduction, which is completely entangled with the profession" (Digitalization director, February 2019)

By the end of the episode, the department of family care decided on development of a new communication platform SecureDialogue which could be downloaded as a mobile app. When opening the app for the first time, foster parents would log in with their NemID and consequently provide appropriate legal permissions for exchanging sensitive data about foster children. Subsequently, the app functioned like other instant messaging services; previous conversations between caseworkers and foster parents were easily accessible and sending notes, pictures and video mimicked similar functions associated with normal text messaging. While the solution was developed by an external company, a developer from Fairview's own IT and Digitalization department functioned as the primary point of contact, which meant the chosen solution was eventually implemented in two other departments; the competence center and the Substance Abuse Rehabilitation Center.

> "SecureDialogue will be a joint resolution for several departments, so that the same solution works across the municipality. Often, there is a need for interaction outside e-Boks with some citizens, and there is an urgent need to

> support this with a technical solution. Foster families must communicate with the municipality and they are obligated to report at least twice a year, which was sent in a Word document, on their private computers, which was a no go." (Information security coordinator, April 2019)

As competing concerns were resolved by the end of episode #3, the Digitalization director had activated collective participation and expressly entrusted the practitioners closest to the foster care practice with devising appropriate arrangements. The data venture originally materialized as the Information security coordinator was asked to help resolve a formal compliance issue but had progressively evolved to involve multiple strategic, managerial, operational and material activities which resulted in a new technical resolution for multiple departments and adapted communication practices between foster parents and family care consultants.

5.4.4. EPISODE SUMMARY

The third episode *Activating collective participation* unfolded in extension of episode #2, as concerns for data as a collective resource had moved to the forefront in Fairview. After experimenting with different strategies for devising data governance arrangements for GDPR, the Information security coordinator had improvised a new type of action arena; the data venture. These experiences had illuminated the importance of actively including practitioners in negotiating resolutions between abstract data protection policies and their local work practices. Episode #3 therefore focused on activating collective participation across different initiatives to improve support for data governance arrangements. Threats to collective action were consequently exacerbated as data practices were deeply embedded in local work practices and therefore required input and cooperation from practitioners.

What signaled the end of episode #3 was the conception of the first formal, organization-wide data governance arrangement in Fairview, directly addressing data as a collective resource and not an IT architectural issue or a directly mandated GDPR initiative. The guideline for handling personal data in Outlook calendar entries essentially addressed a very bounded area, but it brought concerns for data as a collective resource in Fairview to the forefront and simultaneously illustrated the extreme complexities involved in devising arrangements that were both multilateral and congruent enough with local conditions to ensure participation.

At the outset of the episode, entanglement of data practices with local work practices was considered a potential threat to collective participation, because determining lawful bases for data processing and thus for devising appropriate governance arrangements depended on deep, contextual knowledge of legally mandated municipal domain responsibilities, IT architecture and data protection regulation. Since the Information security coordinator and the Digitalization director were devising most arrangements, they lacked this necessary contextual knowledge to understand whether rules would be appropriate. After actively leveraging organizational responses from practitioners in

Fairview, a supplemental instruction was published to make rules more congruent with local conditions and thus mobilize support for the arrangement.

5.4.4.1 Highlights from Episode #3:

- Focal actors were Information security coordinator with the Digitalization director, who were no longer only doing background work, such as producing formal documentation and mapping IT systems; they engaged practitioners to adapt operational rules
- Data processing was difficult to separate from work routines, specifically illustrating how devising data governance arrangements were about changing existing operational situations, and not about supplying a whole new set of general rules
- Attempts to devise multilateral arrangements prompted new activities for regulating the boundaries of the resource systems, including defining who had access to which data, how and why, which involved multiple considerations of group memberships, social norms, physical localities, and digital solutions
- Attempts to form operation rules for calendar entries which appeared universal in Fairview were met with resistance, since these rules were not devised in appropriate collective-choice arenas and thus were not congruent enough with local conditions
- A third data venture was brought into being to cope with competing concerns in the entanglement of data protection regulation, operational rules for data processing, outward bound communication practices with foster parents and existing digital practices all closely tied to local conditions
- Resolving the third data venture involved highly specific operational rules to facilitate data processing outside boundaries of the resource system, and was supported by adapting existing communication practices and developing a new digital solution

5.5. EPISODE #4: NESTING DATA GOVERNANCE IN MULTIPLE LAYERS

APRIL 2019-JUNE 2019

By April 2019, most resources in Fairview had been directed at devising formal arrangements, like template documentation, a central system overview, general guidelines and generic education in information security. As uncertainties about whether public authorities would unexpectedly arrive to audit formal data governance arrangements in Fairview dissipated, attention shifted towards affecting sustainable change to work practices involving data use. Experiences with data ventures showed they functioned well as intermediate action arenas at collective choice level, where practitioners could actively be involved in negotiating tensions between deeper constitutional rules and local operational rules. As the Information security coordinator had discovered during formation of the Outlook guideline, realizing new rules, however actionable they were, would still require continuous adaptations and translations when confronted with the many complexities of professional routines.

At the beginning of episode #4, negotiating resolutions in this manner was considered unstructured and ad hoc. Yet, as the episode progressed, a shift in perspective eventually enabled the Information security coordinator to leverage and coordinate localized organizing. She focused on empowering practitioners to devise their own small-scale, situated data governance arrangements to cope with conflicts in relevant operational situations.

Previous efforts in Fairview had mainly been directed by an external standard for information security because GDPR offered little actionable guidance for how to devise and incorporate the many data governance arrangements in practice. While the ISO standard functioned as a set of guiding principles, the monocentric, hierarchical organizing logic imposed by its normative approach proved incompatible with Fairview's self-governance and local autonomy. During the final episode, the Information security coordinator worked to strike a new balance between planning less initiatives in advance and addressing more problems as they became prominent:

> "[We try] to find a solution that works in practice because one thing is maybe what we sit and think in here, but how does it actually work out there? What do they need? I just believe a lot more in that approach, where you take it up when it occurs and maybe you think you're staggering a bit and things feel a little unplanned, but […] it also achieves such a snowball effect" (Information security coordinator, June 2019)

Instead of only focusing on devising organization-wide arrangements, the Information security coordinator accepted that progressively attending to smaller, local issues with practitioners would eventually amount to greater results.

Until the onset of episode #4, the Information security coordinator and the Digitalization director had evolved an intricate set of polycentric organizing patterns. They had continuously established and readjusted boundaries for the common data resource system in Fairview; arranged intricate monitoring and sanctioning practices; improvised and experimented with data ventures as a new action arena for dealing with emerging issues; and facilitated collective choice by engaging practitioners in forming new rules. Yet, as they continued to address competing concerns for data use in practice, social norms of reciprocity and mutual accommodation proved critical to devise sustainable resolutions between general rules and local conditions. Rather than seeking minimal coalitions for broad arrangements across Fairview, where self-governance was dominant, the two focal actors focused on establishing robust arrangements in smaller coalitions of practitioners with strong social ties. They then nested these many arrangements in multiple layers to progressively cover the entire organization.

5.5.1. COLLECTIVE ACTION THREATS

During previous episodes, the Information security coordinator and the Digitalization director had established intricate organizing patterns to address emerging issues, but resolution of these tensions were primarily addressed in order to devise general arrangements involving all departments in Fairview, such as the Outlook guideline. As the rules for data processing were meant to encompass the broadest possible representation of practitioners, such data governance arrangements simultaneously neglected social norms of reciprocity in local professional practices and remained incongruent with day-to-day operations, which posed significant threats to collective action.

5.5.1.1 General arrangements remain incongruent with local conditions

Despite devising an actionable guideline for handling sensitive data in Outlook calendar entries, the Information security coordinator continued to receive questions of very specific character. Even though she had constructively leveraged feedback and organizational responses from practitioners in reshaping rules, many practitioners were still in doubt about how exactly to adhere to them in their specific domain. Upon release of the final supplemental instruction, the coordinator was first invited to present the guidelines and answer domain specific questions for the management group in department of Children and Youth, because they had received numerous questions from social workers, special consultants and counselors that they were unable to answer. By the end of the presentation, which focused on relaying the guideline and dispelling myths about control and travel reimbursements, the executive director for Children and Youth still concluded:

> "I think it would be good for our employees to see this presentation themselves. So they can ask have I understood it correctly in relation to my own practice? How is what visible to whom? What about communication

> with external parties? (…) so they understand the balance between 'such is the rules' and 'we know it is difficult"' (Executive director for Children and Youth, April 2019)

Even after the Information security coordinator had mediated the general arrangement for management within children and youth social services, it was not enough to be considered actionable. According to the director, the rules still needed to be renegotiated directly with individual practitioners, in response to their specific questions, so they would feel their qualms and confusions had been met with understanding, even if they still had to adapt to inconvenient practices.

As the Information security coordinator held the exact same presentation for 10 selected practitioners from the department, new complexities resurfaced. Multiple different professions were represented among the 10 participants, including a pediatric nurse, a physiotherapist, a special consultant, a social worker, a manager from pedagogical-psychological counseling, the department secretary and the executive director for children and youth. During the presentation, questions from participants illustrated how the many different professions working together under different legal bases in a decentralized IT landscape resulted in multiple competing concerns for sharing data. Access to case files were limited by strict IT access control mandated by national laws governing the individual municipal responsibilities. In one example, it was not possible for the pedagogical-psychological counselor to devise a cohesive treatment plan for a child, because it depended on consulting an inaccessible action plan written by the pediatric nurse in her IT system. Exchanging sensitive, confidential data across disciplines formed the basis of most social work in the department, but since IT systems did not allow secure exchange of data, the practitioners resorted to Outlook as a cross-functional coordination tool:

Exec. Dir.: "You really must not write confidential data in the note field. It has always been illegal, but now we must comply with it. Using these data must always be determined by the specific purpose. It is not about 'as much data as possible', but about why you write it down"

Social worker: "But what about unit management and internal confidentiality? There are many different disciplines here in [children and youth] with many different systems. We can't even link to cases and we don't work in the same professional systems, it's a challenge."

Inf.Sec.Coord.: "No, it still doesn't work. It is the specific context and not the department that decides what can be written. Note, subject, place. The last two are open and if you really need to receive more information, you have to pick up the phone and ask for it. I know it needs to work in practice, but then we have to live with this until another [cross-functional IT] solution comes along"

(Outlook guideline presentation for Department of Children and Youth, April 2019)

Within interdisciplinary, municipal professions, unit management and confidentiality referred to a practice, where practitioners could legally share sensitive data among them to address cross-functional cases. If a child placed in foster care also received support for health-related issues, then family care consultants and pediatric nurses collaborated to put together a broad treatment plan. Yet, a central prerogative of GDPR meant data processing was sanctioned under specific, contextual conditions in order to prevent data collected under one purview from being illicitly reappropriated for other purposes without the data subject's knowledge. Even if the specific instances of data sharing between professions were legal, it would still have to be determined on a case to case basis, not by default. Irrespective, Outlook still did not meet technical requirements, and the Information security coordinator emphasized that cross-functional data exchanges therefore needed to take place in other forms, such as over the phone, even if this was impractical.

Following multiple of these presentations, including a similar setup for department of Elder and Disability, the Information security coordinator acknowledged that nearly any type of overarching arrangement would produce similar outcomes:

> "Processes go across, so it solves the problem when something moves out of 'my' system, but processes are also fluffy to work with. How detailed should it be? [Onboarding in human resources] as a process may seem clearly definable, but in reality, it is enormously difficult to work with. Sometimes, it's a straightforward process, but most work areas have all sorts of branches and there are many different systems within what appears as one process". (Information security coordinator, April 2019)

Entertaining the idea of devising data governance arrangements for processes (as opposed to systems), which would support many of the concerns raised by social workers, the Information security coordinator did not see a way around negotiating situated resolutions. Even work processes would involve local exceptions.

What had appeared as a simple, actionable guideline continued to prompt situated renegotiations and reveal seemingly irresolvable competing concerns when meshed with local operations. Even if previous efforts by the Information security coordinator and the Digitalization director had readjusted boundaries for sensitive data as a collective resource and activated collective choice to define meeting types across Fairview, they had not eliminated incongruences between de jure rules imposed by general arrangements

and de facto rules used in practice[15]. At the outset of the episode, the incongruences between general and local rules posed threats to collective action.

5.5.1.2 Neglecting social norms of reciprocity

Until now, nearly all efforts to devise data governance arrangements had been driven by the Information security coordinator and the Digitalization director. Familiar with the Fairview model, the two focal actors had gone to great lengths to accommodate contractors' autonomy and local department practices, even though information security practices and GDPR compliance were inherently normative. Experiences with devising and implementing the Outlook calendar guideline had essentially focused on imposing a general rule without making it feel as such. Any resistance to normative concerns for data had been addressed by the IT and Digitalization department by enacting polycentric governance, for example through collective choice, but the Digitalization director was still keen on remaining a central, coordinating unit:

> "We are a little like this in IT and digitalization, where we want to get involved before they buy [IT systems] because it's us who have to solve the problems afterwards when the systems can't talk to each other and don't comply with security requirements and such, but they are actually allowed [to do that], so it's a challenge to come from a central place and say 'now things have to be done this way and that way'. We're still trying to find our legs in this" (Digitalization director, April 2019)

Unremitting renegotiation between general arrangements conceived by the IT and Digitalization department and local operational rules were seen as a hurdle to be overcome with time. Devising new arrangements had focused on communicating normative concerns for data and information security in a manner that resonated with existing social norms for work and professional conduct within the individual departments:

> "We're actually doing it for the sake of the citizens; we're not doing it for the data protection agency or as an obstacle to be overcome or to make it difficult for you to do your job as a social worker, [but] that is also what makes it so difficult to communicate, because it's a slightly more fluffy goal, and in 99% of the cases, nothing happens. There are no dead and wounded, when you make a mistake processing sensitive data, so it can be difficult to set it up against treating the disabled and helping vulnerable citizens, that it should be so important" (Information security coordinator, April 2019)

---

[15] de jure refers to practices that are legally sanctioned, even if they are not exercised by anyone in practice, while de facto refers to what is actually exercised in practice, even if not legally sanctioned as rules

New directives set by GDPR mandated formal arrangements of the kind the Information security coordinator was advocating for. Yet, experiences from early data ventures also showed that non-IT practitioners were in fact cooperative and eager to negotiate effective compromises, if only it was done close to their reality and with appreciation for the work they were doing. An outcome like the PDF cleansing tool (see section 5.3.3) resulted not from arrangements devised by the IT and Digitalization department or sanctions imposed by the Data Protection Agency, but from practitioners in Technical and Environmental Services seeking a sustainable agreement between performing their own work and ensuring positive citizen experience with local government. The SecureDialogue solution (see section 5.4.3) was also the outcome of dedicated social workers looking to reshape communication practices with foster parents to support secure exchange of data, which unexpectedly also proved to be a concern for social workers in the Substance Abuse Rehabilitation Center and the vulnerable youth department. Meanwhile, these dynamics were not immediately perceived successful accomplishments to the Information security coordinator:

> "The scope [of our initiatives] really should be greater, but the basic level is that we try to avoid illegal actions. There are alternative solutions to all these problems, but the question is always how do we make sure tasks can be solved compliant and legally" (Information security coordinator, April 2019)

Contrary to resolutions from previous data ventures, which had evolved to address competing concerns between compliance and operations but ended up providing additional value, the Information security coordinator still saw these as isolated initiatives on the path toward baseline compliance. Despite actively engaging practitioners to devise meaningful arrangements in previous episodes, the role of social norms for reciprocity in these resolutions were largely neglected in the efforts by the Digitalization director and the Information security coordinator to devise data governance arrangements. This posed threats to collective action at the outset of episode #4.

5.5.2. ENACTING POLYCENTRIC GOVERNANCE

Throughout previous episodes, polycentric governance had brought data ventures into being as intermediate action arenas, where the Information security coordinator negotiated resolutions for competing concerns as they became prominent in practice. Until this point, these temporary arenas were not considered very constructive, but rather time-consuming, isolated incidents; messy and disorganized, even if they accomplished effective outcomes:

> "There is no organization and it is very ad hoc. An interdisciplinary team or something like that would be optimal, because right now, [the other practitioners] do not have to work together, or to work with me. Issues continue to emerge from all sort of different places all the time, and it takes resources and energy to resolve each of them" (Information security coordinator, February 2019)

Data ventures unfolded outside and between established hierarchies and involved no clear definition of roles and responsibilities. Resolutions were negotiated in response to unexpected issues, but it took resources and involved multiple practitioners from different professional backgrounds, who had no formalized obligation to contribute. Since social norms of reciprocity and mutual accommodation were not at the forefront at first, the coordinator seemed to work from the assumption that contributions from practitioners could not necessarily be expected going forward and therefore needed to be enforced in a team structure.

As the episode progressed, advancing carefully planned, organization-wide arrangements became increasingly difficult, since fears of harsh sanctions were beginning to dissipate. Instead, issues in specific work practices continued to reemerge and require the attention of the entire IT and Digitalization department, who persistently negotiated new situated resolutions every time. Many of the polycentric organizing patterns enacted by the Information security coordinator and Digitalization director to devise common rules at organizational level for several heterogenous professions, practitioners and processes were also observed in the forming of small-scale data governance arrangements. They were enacted between smaller groups of practitioners, who knew each other well and had deep appreciation for the working context. When the responsibility for devising small-scale arrangements was devolved to smaller groups of practitioners, the resulting rules were not only congruent with both local conditions and existing general rules, but also adopted with much less resistance, confusion and renegotiation than the broad arrangements sought by the Information security coordinator.

Consequently, while the Information security coordinator and other practitioners from the IT and Digitalization department remained focal actors in the episode, polycentric governance was enacted in a distributed manner, shifting attention to cultivation of social ties with non-IT practitioners in Fairview. Ultimately, the Information security coordinator accepted progressively defining rules in response to emerging problems was in fact the most productive – not just an unplanned – approach to devising data governance arrangements, which could be leveraging nested by leveraging multiple action arenas at different levels.

5.5.2.1 Shifting attention to social ties

Previous episodes had seen varied digital maturity, heterogenous concerns for data, resistance to normative approaches and friction between central authority and local autonomy as threats to collective action for organization-wide data governance. These issues also seemed to diminish when issues were negotiated through collective choice in emergent data ventures.

For the Outlook guideline, the Information security coordinator had intently pursued instructions which were concrete and populated by real examples from various scenarios in Fairview, first believing this would make the guideline easier to adhere to. Yet, as she

continued to receive requests for presenting the guideline and answering specific questions, negotiating these local resolutions seemed to be less about the outcome and more about the social process of brokering compromises with practitioners.

Meanwhile, a Business developer and a Digitalization consultant from the IT and Digitalization department working with Robot Process Automation (RPA) had experienced firsthand how important establishing social ties with and between practitioners were for devising arrangements involving data. While their work with RPA focused on modeling simple, repeatable administrative tasks and turning them into automatable workflows to be performed by metaphorical software robots, they often had to address social issues:

> "You can't come down there, when they can't figure out how to talk to each other. Sometimes we land in a gap between an HR task and a process optimization task. We have to consider whether it's a problem that stems from sluggish workflows or that people can't talk to each other […] because when we're asked to do something, it's either because the managers don't know it exists or because they think they can solve it [with a robot]. We often fall into that and sometimes, we have to say, 'listen up, this has nothing to do with your workflows'" (Business developer, April 2019)

Shifting attention to social dynamics within a team was crucial for developing effective RPA solutions. Practitioners were essentially asked to model their own workflows to enable a software robot to assume certain menial tasks, so time and resources could be reallocated for other creative, developmental tasks. In turn, this required mutual reciprocity and significant trust between the developer and the practitioner:

> "When you develop these robots, […] it's very much about moving employees from doing some routine tasks to doing some more exciting, developmental tasks, and it's about increasing efficiency, because a robot inevitably manages more tasks than a human or a caseworker does. We often encounter this dilemma, but we do a lot to articulate that it's a short-term thing. When people come in, we don't want them to feel like they're creating the foundation for being fired, because that makes no sense" (Business developer, April 2019)

During the workflow modeling process, cultivating understanding for the 'why' was ultimately more important than the 'what', even though implementing a software robot meant eliminating menial data processing tasks. If practitioners had not understood why relinquishing certain assignments would be mutually beneficial or felt their position was threatened, they were unlikely to provide the necessary insight needed to devise an effective automated data processing workflow. Consequently, the Business developer and the Digitalization consultant paid substantial attention to social ties and invested in building rapport with practitioners:

> "It's about the very basics, about having a dialogue, being open and listening, these are some personal competencies that must be in a team, for this to work […] when it becomes simple and straightforward and it makes sense, then [practitioners] actually start to relate to data themselves […] it's not a question of competencies, as in that you have to have a course in statistics, it's more this connection with 'how does it make sense for what I'm working with now?" (Digitalization consultant, April 2019)

Experiences from developing RPA solutions illustrated similar patterns to previous data ventures. Negotiating resolutions between competing concerns for data as a collective resource, whether in a software robot or a rule about calendar entries, depended more on establishing social norms of reciprocity, trust, and sincere appreciation for how practitioners were performing their job than on high digital maturity, dedicated data analytical competences or technical know-how.

As RPA development often coincided with questions about whether certain data were affected by GDPR, the Information security coordinator frequently provided input about specific issues to the Business developer and the Digitalization consultant:

> "We use [the Information security coordinator] and sometimes we all three sit with it, with data from the control language we have to bring forward (…) The thing with GDPR is that you can't really say anything general, it's often that departments bring something specific, like 'where can we store these data, like lists of students in a class'" (Business developer, April 2019)

As episode #4 progressed, the Information security coordinator not only shifted her attention toward cultivating social ties, but actively sought to empower individual practitioners to devise data governance arrangements congruent with their own operational rules:

> "The foundation and formal decision-making structures are in place, but for awareness, it's a process of gradual maturity. There are still many discussion points and unanswered questions from practitioners. 'What is the meaning of a data processor agreement? How do I read an auditors' statements?' My responsibility is to educate them locally, so that they become self-sufficient because with freedom comes responsibility." (Information security coordinator, April 2019)

The shift in attention marked a significant evolution for how polycentric governance was enacted. Around the formal instatement date for GDPR in May 2018, all work on devising data governance arrangements in Fairview had focused on producing data processor agreements and auditor statements for IT systems. Since failure to document compliance was sanctioned just as hardly as actual violations, the Information security coordinator had prioritized producing documentation rather than educating local system owners about the meaning and purpose of such arrangements. In episode #3, this had

resulted in tensions between collective concerns for data and localized work practices, because neither official authorities nor the Information security coordinator had enough domain knowledge to devise appropriate rules for large professional IT systems, while practitioners lacked sufficient understanding of how to interpret data protection regulations to devise these rules themselves (see section 5.4.1.1). By episode #4, the perspective had shifted, and the Information security coordinator now understood that formal structures needed to be complemented by general awareness, which could only be developed by increasing the authority of individual practitioners to devise their own rules.

5.5.2.1 Addressing tensions progressively as they become salient

While progress slowed on larger organization-wide initiatives, the Information security coordinator simultaneously continued to receive various questions about how to address specific issues in practice. As a result of the elaborate monitoring and sanctioning practices arranged in episode #2, practitioners were also not afraid to direct inquiries about violations, which often meant the coordinator had to reprioritize to resolve urgent problems as they were reported, instead of moving larger initiatives ahead. Previously, she had referred to this as messy and unorganized, but it had also become harder to ignore the results:

> "Sitting down, trying to think 'what could we do here', it would be such a waste, plus we shouldn't underestimate the effect from those who ask for help themselves […] you really have to take them seriously [and] find solutions there quickly, rather than trying to find solutions for everything everywhere at once. You can't do that and then you end up wasting time, so to speak, because there will be some practitioners who are just not ready yet" (Information security coordinator, April 2019)

Instead of planning arrangements based on assumptions about how to resolve presumably inadequate practice, the Information security coordinator acknowledged that resources were best spent resolving tensions that had already become salient. In turn, she circumvented a problem she had first encountered, when conceiving the organization-wide rule for Outlook calendar entries, namely that no matter how actionable a general arrangement was, it would still require multiple, local renegotiations. With time, the coordinator had not only learned that she lacked sufficient domain knowledge to be able to proactively confront tensions, before they emerged, but also that data governance arrangements were more congruent with the local conditions, when they had been devised in response to specific concerns arising from local conditions.

One such example unfolded midway through episode #4, where the IT and Digitalization department by chance discovered emerging tensions in communication practices between an elementary school secretariat and parents of children about to enter preschool. An IT developer had received an email from the secretary at his daughter's coming preschool, asking all parents to please fill out a form with various, potentially

sensitive information about their child, such as whether they had seen a psychologist, who their siblings were and any history of mental or physical illness. Not only was the email sent to all parents, whose email addresses were fully visible to all receivers, but it also encouraged them to return the completed form by email to the secretary. The developer reacted immediately. Proprietary email clients, like Outlook, Hotmail or Gmail did not meet security requirements, which meant the correct process would involve returning the document through the secure communication platform e-Boks, but the email did not specify to do so. Moreover, using e-Boks to communicate with the school was by no means straightforward, increasing the risk of mistakenly directing sensitive data to the wrong department:

> "It's a dropdown menu, where you first have to find your municipality and then you have to find the recipient, and if it is within some subject area, which has 3-4 different email addresses, which makes it easier for us here internally, the citizen must choose one of them with the danger of choosing the wrong one too" (IT developer, April 2019)

Processing sensitive data in this manner was by far GDPR compliant, but it also only came to the attention of the Information security coordinator by accident because her colleague in the IT and Digitalization department coincidentally had a daughter about to start preschool. Even if the coordinator had planned a vague initiative looking to examine communication practices between school secretaries and parents, the initial problems were important pointers for shaping new rules congruent with local conditions:

> "We could probably have sat down and said now 'let's look at school communication with parents' [but] there are just some dynamics that become completely clear when they arise from practice. Such as what's the main core of the problem? How does the simplest solution look? Similar to the incident with foster families, like no, they don't need to have a computer from us. You might be tempted to come up with that, if you were sitting behind the desk and had to think your way to a solution" (Information security coordinator, April 2019)

The change in perspective again signaled significant evolution of polycentric governance in Fairview. While negotiating competing concerns as they materialized in practice was considered ad hoc and disorganized to the Information security coordinator in February 2019, her experiences with situated resolutions indicated that addressing emerging tensions was not only inevitable, but also conducive to devising effective rules. In fact, mobilizing collective support with a group of practitioners was considered easier, if data governance arrangements had been devised in response to specific competing concerns emerging from their own day-to-day routines:

> "The awareness you achieve, I don't think you should underestimate that, because rather than coming up with some desk project, we have devised and decided to roll out, like 'now this is important to you', it doesn't work. You

> don't get people onboard with that. They take responsibility in a completely different way from the start because [the arrangement] originated from their own everyday life, and instead of having to first accept the premise for why something is problematic and then afterwards the solution, they already have it under their skin why they need to do something differently" (Information security coordinator, April 2019)

After experimenting with different strategies for devising rules and facilitating collective choice in the past episodes, the Information security coordinator had learnt that if practitioners in Fairview were allowed sufficient independence to shape and enforce rules for a bounded domain in the common data resource system, in response to specific competing concerns arising from their own particular practices, resulting data governance outcomes would be substantially more congruent with local conditions than any central 'desk projects'. Devising small-scale arrangements allowed fewer practitioners to develop social norms of reciprocity, trust and sincere appreciation, which would enhance cooperative behavior and facilitate accommodating resolutions, eventually reducing threats to collective action. Empowering practitioners to leverage their social ties and localized knowledge about conditions allowed for quick experimentation and feedback about resolutions, while centrally coordinated 'desk projects' lacked local anchorage and moved slowly.

Finally, addressing tensions as they became salient in specific competing concerns also enabled the Information security coordinator to distribute accountability for experimenting with rules across multiple bounded arrangements, rather than relying only on a single, central authority to experiment with appropriate solutions for organization-wide rules. Allocating rules within multiple, relatively separate data governance arrangements would reduce the risk of complete failure, if any errors occurred.

5.5.2.2 Leveraging multiple organizational levels to nest governance arrangements in layers

When the Information security coordinator first began to devise data governance for GDPR compliance, she referred to much of her work as 'inventing a new level' (see section 5.3.2.1). At the time, moving between abstract rules for data protection and specific issues in practice were seen as transitional toward arriving at a final 'level', where general arrangements could be devised for all practitioners in Fairview. After recognizing the permanent need for brokering local resolutions following the Outlook guideline, the coordinator instead began to consider how situated resolutions could be nested in layers across organizational levels:

> "Kitos is an organization-wide tool that provides an opportunity to look down from above. SecureDialogue is an example of top and bottom meeting each other. Progress on the large initiatives is much slower than on the small initiatives, which are quickly implemented. We can resolve some small, specific tasks, but the plan is to enable system owners to address the

> remaining shortcomings, since it often starts with the specific which then becomes something much bigger (Information security coordinator, April 2019

Affording system owners more autonomy to devise operational rules within their domains would enable faster progress, in the sense that previous, emerging data ventures had allowed quicker resolution of competing concerns, than large-scale preplanned initiatives had. The Information security coordinator also recognized that some specific issues emerging from practice could potentially necessitate broader resolutions. Instead of directly pursuing large-scale arrangements at one organizational level, she sought to progressively rules for bounded arrangements until there would be an overlap, similar to how the solution SecureDialogue had started from a specific local issue, but eventually evolved into a multilateral arrangement between several departments.

Prior to GDPR, Fairview was making use of system owners as a decentralized arrangement for distributing accountability for domain-oriented IT systems. System owners were designated practitioners, often team managers in Fairview, who were also responsible for (one or more) IT systems, including determining appropriate use of the systems in domain work, setting common directions for data processing and training new employees in using the systems. During preliminary work to the define boundaries for a common data resource system in Fairview (see section 5.3.2.1), a series of Kitos responsible had been formally designated to make sure system owners registered their systems within the tool.

As earlier tensions had indicated (see section 5.4.1.1), the Digitalization director and the Information security coordinator eventually realized maintaining Kitos entries required a deep appreciation for both the IT systems in question, their working municipal context and the data protection regulation. System owners had both IT system expertise and contextual domain knowledge and were already involved in updating data processing agreements and GDPR mandated risk and impact assessments for IT systems containing personal or sensitive data. Rather than maintaining a full, separate governance structure just for producing formal documentation in Kitos which required domain knowledge anyway, it was decided to devolve more responsibility for maintaining system entries in Kitos directly to system owners.

Although this responsibility had been relayed to system owners, no initiative had been taken to follow up on how it was adhered to:

> "There is this issue still to be resolved, which is that the system owner must live up to their responsibility in practice and not just on paper. There are different concerns that need to be documented and rules that need to be in place. Of course, it's something that has been communicated, everyone has received this A4 page with system owners' tasks and responsibilities on it, but we haven't taken any initiatives to say 'now things must be finished' and we

> need to check whether [the system owners] have the documentation that there needs to be" (Information security coordinator, April 2019)

Simultaneously, by the end of the final episode, the coordinator was planning a prospective audit with Fairview's DPO. Since preparing for an official audit by the Data Protection Agency required substantial large-scale initiatives, efforts and resources from a municipality, the DPO suggested strategically choosing a theme which would create value in Fairview beyond demonstrating formal compliance:

> "Different themes may come up during an inspection, but I would like us to decide together what to focus on. We need to identify an overlap between areas that are important to Fairview, so that it can be embedded in the audit, so you get value besides just control. We can focus on initiatives you need legitimized in the organization, by saying 'the DPO has determined this' so that it is taken seriously." (DPO, April 2019)

The DPO considered this a strategic opportunity to provide legitimacy to general arrangements in Fairview which were otherwise hard to mobilize collective support for. Fears about harsh sanctions had slowly dissipated since May 2018, but the prospect of a formal audit could likely reinvigorate incentives for participation in collective arrangements. Since the coordinator wanted to mobilize system owners to enact their formally defined responsibilities in practice, it was a fitting theme for the formal audit. To the DPO, focusing on system owners was also well-aligned with broader concerns:

> "I think this is a theme that can last a long time. The Danish Data Protection Agency is not satisfied with Local Government Denmark's proposition, so we should focus on showing the quality of our work to the outside. [Fairview's] work with Kitos and the system overview is far ahead compared to other municipalities. We should go crisscrossing in Kitos, to show it as the good example, and show how data processing and access are under control" (DPO, April 2019)

Fairview kept an external lawyer on retainer as their DPO, which meant he was continuously getting input from other municipalities through colleagues working as DPOs in other municipalities. Moreover, he was formally accountable to the Data Protection Agency. The agency had not been satisfied with the municipal association Local Government Denmark's formal guidelines for maintaining an overview and the DPO felt it was inadequate compared to the work already accomplished by Fairview, who used the open source tool Kitos. Showcasing the overview in Kitos would be ideal for the audit, as it would both demonstrate higher levels of compliance than expected from average municipal standards and provide leverage to instruct system owners about their responsibilities:

Inf. Sec. Coord.: "How should the audit be timed with the workshop for Kitos responsibilities? It is important to ensure lasting anchorage with

system owners and it is important to get through all systems that contain personal data."

DPO: "We can focus on self-assessment to create support and say: 'there may be a knock on the door'. System owners will be equipped in practice to handle their own systems (...) They must relate to personal data terminology in order to determine who gets access to what on which criteria, and they must know their employees and regulation. Why can some access certain data? It requires a basic understanding [and] training for them to know about their own 'shop'."

(Coordination meeting, DPO and Information security coordinator, April 2019)

For the Information security coordinator, it was important to empower system owners in the long term; not just produce more formal arrangements. Yet, she also wanted to ensure Fairview did not fail the inspection, because system owners had misrepresented their systems in the overview. In response, the DPO suggested a resolution, where system owners would be trained to self-assess their systems, with a basic understanding of both the data protection regulation and the legal bases under which practitioners within their municipal domain were allowed to process sensitive or personal data. Instead of approaching it as a compliance audit, the DPO proposed letting system owners know there could potentially be an official inspection, a 'knock on the door' from authorities, but that the main purpose was to make them experts in data regulation for their own domains.

In May 2019, all system owners and system administrators[16] in Fairview first participated in a generic course on how to read external auditors' statements for an IT system hosted by an external consultancy. An auditor statement was a formal review of a data processing agreement performed by a lawyer, and either certified that data processing for a given IT systems was legal under specific purviews of the GDPR or pointed to any discrepancies, violations or ambiguities, which needed to be amended. Following the generic course, the IT and Digitalization department hosted an internal workshop for the same participants, which focused on an overall review of system owners' areas of responsibility, and group sessions, where system owners could get help to review and document governance arrangements for user management and access control in their domain-specific IT systems.

By the end of the final episode, devising data governance arrangements in Fairview was no longer only a centrally coordinated effort by the IT and Digitalization department. On one level, system owners were both formally obligated to maintain formal entries about data governance for their IT systems in Kitos and practically responsible for negotiating situated resolutions between general rules for data protection and local work practices

[16] Corresponding IT supporter responsible for technical operations of IT systems

involving data. On another level, the IT and Digitalization department used the overview in Kitos to formally monitor data governance arrangements and make sure risk and impact assessments, data processing agreements, auditor statements and KLE identifiers[17] were in place for all IT systems in Fairview. Consequently, rules were both congruent with local conditions and formalized in an overview, which made monitoring and sanctioning infractions easier.

On a higher level, the DPO had considered the overview advanced and promising for demonstrating compliance upon inspection by public authorities in Fairview. In preparing for the audit, the DPO and the Information security coordinator essentially negotiated large-scale resolutions between organization-wide arrangements in Fairview and national regulations upheld by the Data Protection Agency, which eventually resulted in the workshops for system owners. As a result, local rules devised by practitioners were nested in another set of organization-wide rules for registering formal arrangements, which were then nested in a broader set of nation-wide rules for how to demonstrate compliance in official audits.

As data governance arrangements were nested in these layers, they were also more robust in an organization like Fairview, where local self-governance was important, but working with data as a collective resource was still foreign to many:

> "We try to establish the necessary organizational maturity for working with [data governance] by paying attention to what happens where and the shifts between organizational levels. At some point, it will reach a point of saturation. They come to us when they have an issue, so it comes to them in doses when they need it and then we try to oversee compliance on something that provides value to the organization" (Information security coordinator, April 2019)

Where the Information security coordinator had succeeded in mobilizing collective participation in episode #3, she had managed to distribute accountability for devising data governance arrangements at multiple organizational levels by the end of episode #4. Allowing practitioners with deep contextual knowledge and shared social norms, to autonomously define rules in bounded arrangements congruent with their own localized conditions had resulted in more congruent rules. Rather than trying to conceive organization-wide arrangements in advance, which would inevitably require situated resolutions anyway, the Information security coordinator instead sought to progressively nest local rules in multiple layers.

---

[17] KLE identifiers refer to a municipal records management taxonomy developed by Local Government Denmark to connect municipal responsibilities with corresponding obligations mandated in the law

5.5.3. ZOOMING IN

While GDPR formally mandated risk assessments for any IT systems processing sensitive or personal data, there was no official format for undertaking such assessments. The regulation only specified three dimensions for data protection, namely confidentiality (protection against unauthorized access), accessibility (protection against unauthorized access restrictions for persons with authorized access) and integrity (protection against unauthorized alteration or destruction). Consequently, the Danish Data Protection Agency had produced supplemental guidelines, which among other things specified an impact assessment for evaluating the consequences of loss of confidentiality, accessibility or integrity in any IT system processing sensitive or personal data. By the end of episode #4, tensions manifested as an impact assessment had revealed competing concerns for data use in Fairview's competence center.

In Fairview, the competence center aimed to assist unemployed citizens with returning to the job market, and offered a variety of services, including individualized career plans, courses for citizens on unemployment benefits, rehabilitation plans, assistance for long-term sickness leave, subsidized part-time positions etc. As the center often assisted vulnerable persons in returning to the job market, it was not uncommon for social workers to encounter citizens with a history of violence, crime, mental illness, abuse or similar social baggage, which involved potential risks. To protect employees, the competence center had developed a digital tool, where self-harming behavior, depression, aggression and other characteristics could be checked off for a citizen and consequently used to calculate an overall risk assessment in the categories red, yellow or green. If a citizen was designated red, certain measures needed to be taken, such as two social workers for every meeting and no meetings allowed outside official municipal buildings.

According to the Information security coordinator, concerns for the tool were complex and hard to address. For the impact assessment, Fairview had to account for multiple considerations to ensure protection of the data subject's rights:

> "The core of these considerations is, based on what legal purview are we assessing these citizens? How do we state that we do? What are the consequences for the individual to be designated as red, yellow or green? How many citizens should we do it on? Is it everyone who walks in the door of the competence center or is it just a very narrow group that we personally know about? What criteria forms this basis?" (Information security coordinator, May 2019)

Defining in legal terms why processing such sensitive data on citizens was necessary in a competence center could not directly be derived from any legal bases in GDPR. When scratching the surface, multiple other complexities emerged, which were not officially accounted for. Issues about how social workers decided whom to evaluate with the tool, how subjective characteristics were measured and where they were recorded in the first place were far from unequivocal:

> "There is often the attitude that data are objective, but they are not (…) Is it self-harming behavior to drink a bottle of wine every weekend, is it a yes or a no, is it from 1 to 100? When should it be ticked? These problems arise very quickly and makes it difficult (…) but you have to be able to do that, it says in the regulation. We must be able to explain so that those affected can understand what is going on inside the 'algorithm' and if we can't do that, then it's a no go" (Information security coordinator, May 2019)

As mandated by GDPR, Fairview was legally required to define and explain exactly how sensitive or personal data were being processed and for what purpose. Otherwise, they had to desist from doing it. At the same time, the Information security coordinator had great sympathy for why such a tool was necessary for caseworkers, even though it was legally in a grey area:

> "Their argument, which I fully understand, is the safety of the employees. They simply need to know what citizen shows up to such a meeting, and this tool can really help them. They reassess citizens every three months, but then opposite them is the data subject who ends up with this 'sentence' or being put in some category which has unforeseen consequences. Maybe nothing extreme, just two social workers showing up to the meeting [but] how does it affect if you apply for other services or in general the way you are met?" (Information security coordinator, May 2019)

If no clear legal basis could be established, then the solution would hypothetically have to desist, but in practice, the tool was developed to perform a critical service to the employees in the competence center. Previous data ventures more or less emerged to address tensions between normative concerns for GDPR and localized work practices, which were eventually resolved through situated resolutions. While competing concerns in this case had materialized during a formally mandated impact assessment, tensions were clearly perceived to be between subjective concerns for individual citizens' privacy and for individual social workers' safety. Resolving these tensions could therefore not immediately be accomplished through situated resolutions between general arrangements and local conditions.

Eventually, the Information security coordinator produced meticulous documentation about which data were being processed, who the data subjects were, for how long data were stored and which measures they had taken to prevent misuse and sent it for review with Fairview's DPO. According to GDPR, new data-centric technologies with intrusive impact on a broader group of citizens had to undergo formal review first by the DPO and then the Data Protection Agency. As the final episode concluded in June 2019, the Information security coordinator still had not received any feedback, but to her, competing concerns like these were on the rise:

> "I also think it has something to do with the fact that (…) before we used data on something that could be measured and counted. Finances and

> potholes in the road and number of students in a school. Now, it comes down to the individual level and more subjective conditions (…) you have to ask yourself these questions and you have to be able to answer all of them, otherwise you're on a slippery slope (…) Can we really use it for all the things we want to? It's so enticing that we have a lot of data now, but do they really show what we think they're showing?" (Information security coordinator, May 2019)

Previous resolutions for data ventures had focused on devising rules to prevent illicit sharing of clearly defined data resource, such as social security numbers, citizen addresses, e-mails and other data, which were sensitive under certain contextual conditions. According to the Information security coordinator, concerns for new data were not immediately quantifiable, which meant devising rules through meticulous negotiation and mutual accommodation would only become more important to resolve growing tensions between individual and subjective conditions.

5.5.4. EPISODE SUMMARY

The final episode *Nesting data governance in multiple layers* unfolded in extension of episode #3, as collective participation for governing data in a common resource system had been mobilized in Fairview. GDPR had introduced significant changes in a deeper, fundamental set of rules and consequently destabilized existing patterns for organizing data in Fairview. Early anxieties about remaining compliant to avoid harsh sanctions had slowly been absolved by appreciations for the hard work it would take to implement new rules for data in practice. Given the uncertainty associated with such changes, practitioners were cautious and looked to adopt these rules in a manner seen to work for others in similar circumstances. Episode #4 therefore focused on organizing polycentric governance activities in multiple layers of nested arrangements. Threats to continued cooperation were therefore aggravated when general arrangements appears incongruous with local operational rules and the role of social norms were underestimated.

By the end of the episode, the Information security coordinator actively leveraged multiple, different action arenas that she had discovered and experimented with in previous episode, to devise sustainable rules. She moved between arenas such as emergent data ventures, formal Information Security Committee meetings, informal team meetings with practitioners from IT and Digitalization, and coordination meetings with Fairview's external DPO, which afforded her different action opportunities for devising and implementing new data governance arrangements. Rather than pursuing support and input from just one arena at one level, such as the Information Security Committee, the coordinator learned that for a set of rules to remain viable, they needed to comply with exogenous legislation, embrace diverse practitioners moving in various, often diverging professional realities and be negotiated into specific scenarios. Rules that were nested in these multiple layers were more robust, since infractions or disagreements occurring in one layer would not unravel the whole rule system but lead to gradual readjustments. This was exemplified when a GDPR mandated impact assessment revealed competing

concerns for the use of sensitive data in Fairview's competence center. The final data governance arrangement accommodated diverging needs for employees in the center and unemployed citizens and was sanctioned in multiple different arenas, including a formal audit by the DPO and official treatment by the Data Protection Agency. At this point, Fairview municipality worked with polycentric governance by continuously regulating boundaries of a common resource system, enacting effective monitoring and sanctioning practices, fostering trust-based reciprocity in small-scale arrangements and nesting them in supportive large-scale institutions.

5.5.4.1 Highlights from Episode #4

- Although the focal actor was primarily the Information security coordinator, she continuously engaged with various other practitioners in Fairview in emerging collective-choice arenas.
- General governance arrangements attempted to affect change in operational rules by being specific and actionable, but still remained incongruent because it had not been developed in associated collective-choice arenas.
- Despite growing experiences with negotiation in action arenas, it was not immediately clear how social ties and norms of reciprocity were pivotal for achieving congruent rules.
- Cumulative success in small-scale arrangements and relentless renegotiation of general rules eventually convinced the Information security coordinator of the importance in forming rules in collective-choice arrangements.
- Attention was slowly shifted to resolving emerging issues rather than forcing advancement on planned, large-scale initiatives, as specific problems proved instrumental in learning about conditions and moving towards appropriate resolutions.
- The Information security coordinator leveraged multiple collective-choice arenas at different levels at the same time to form rules, while seeking support and legitimacy from large-scale supportive institutions like the Information security committee, the external DPO and formal auditing.
- Emerging tensions for data use in a specifically sensitive context demonstrated growing complexity in resolving inherently competing concerns between citizens and social workers and brought to the forefront acute attention to trust, respect and mutual accommodation in collective-choice arenas.

CHAPTER 6. DISCUSSION

6.1. THEORIZING POLYCENTRIC GOVERNANCE OF DATA VENTURES

Data governance is recognized as a promising and necessary approach for directing the fast-growing, constantly changing set of digital practices involved in organizational data use. Current insights on organizational data use are scattered across diverse research streams but seem increasingly dichotomized by underlying assumptions of techno-optimism and techno-skepticism. Prior studies either imply a fundamentally hopeful outlook on the value and transformative potential of corporate data use or adopt a heavily politicized stance towards datafication of social life which is seen as controversial and inevitably escalating from increased organizational data use (see Table 3 in Chapter 2).

Unfortunately, less than a handful of studies address data governance as both deliberate and emergent organizing of data-related activities and no studies offer integrative understanding or theorizing about how to manage implicated competing concerns as they arise in practice. The objective of this dissertation is therefore to elaborate an organizing logic for data governance that explicates how organizations can engage deliberate and emergent organizing of data use through polycentric governance of data ventures. In the context of a traditional hierarchical organization, this organizing process involves mediating multiple, often diverging perspectives and interests of a wide range of heterogenous stakeholders within and across organizational levels and boundaries.

Drawing on Ostrom's (1990) characterization of robust, self-organizing resource systems to analyze material from a municipal organization over the course of a two-year case study, the dissertation sought to examine how an organizing logic of polycentricity evolves and enables an organization to devise appropriate data governance arrangements in response to competing concerns for data use.

As the empirical foundation for its theorizing, the dissertation examined the case of Fairview municipality in which focal actors progressively enacted polycentric governance to form, adapt, and evolve various data governance arrangements and where multiple data ventures unfolded and were brought into being to resolve competing concerns for data, as they became salient in practice. The theoretical framing allowed the analysis to zoom in and out on organizational processes to capture the interweaving of managerial decisions about the overarching direction for data use with improvised operational choices for how to appropriate specific data sets under local conditions; it also illustrated how social processes of strategizing, coordinating, communicating and interpreting in data-related activities were enmeshed with digital practices of producing and amending material arrangements of data in response to competing concerns.

In the rest of this chapter, key insights from the empirical analysis are leveraged in combination with insights from extant literature to theorize polycentric governance of data ventures and subsequently advance knowledge on data governance. The following two subsections account for the quintessence of the propositioned organizing logic; first, by reestablishing the novel term 'data ventures' as an intellectual vehicle for illuminating the self-rising, situated interweaving of multiple managerial, operational, social and digital practices involved in devising appropriate data governance arrangements; and second, by identifying five organizing patterns of polycentric governance which are progressively enacted to facilitate both deliberate and emergent data governance activities within an existing decision-making structure. The final subsection discusses key implications for such an organizing logic in practice.

6.2. DATA VENTURES

Scholars have recently begun to recognize the limitations of understanding data governance purely in terms of traditional approaches, like formal principles, structures, decision-making rights and asset management (Abraham et al. 2019). Previous research has contributed valuable insights on how to design data governance (Khatri and Brown 2010), but understandings of how day-to-day decision-making unfolds in practice remain unexplored (Alhassan et al. 2016, 2018; Parmiggiani and Grisot 2020). This lack of attention becomes only more problematic, as empirical studies find data governance is difficult in practice (Begg and Caira 2012; Nielsen et al. 2018). Data does not immediately translate to assets for practitioners (Nielsen et al. 2018), but emerge as such when appropriated in situated work practices (Monteiro and Parmiggiani 2019) and everyday data curation activities (Parmiggiani and Grisot 2020). Top-down-driven governance design remains too inflexible for complex, organizational realities (Begg and Caira 2011; Vilminko-Heikkinen et al. 2016a; Vilminko-Heikkinen and Pekkola 2019), where sets of general rules are supposed to encompass a multitude of heterogenous practitioners with diverging professional and ideological perspectives on data (Benfeldt et al. 2020).

To expand this purview, from being just about design to also include everyday data-related activities, this dissertation adopts a broader understanding of data governance as the fast-growing, constantly changing set of digital practices involved in the organizing of data (see section 2.4). Data governance is constantly shaped and reshaped through its ongoing entanglement with a multitude of other formal and informal organizational activities (Monteiro and Parmiggiani 2019; Parmiggiani and Grisot 2020; Vassilakopoulou et al. 2018, 2019). Governing data in practice means interweaving managerial decisions about the overarching direction for data use with improvised operational choices for how to appropriate specific data sets, when performing work under local conditions, restraints and opportunities. It means enmeshing social processes of strategizing, coordinating, communicating and interpreting with numerous technical practices for producing and amending material arrangements of data.

As detailed in section 2.1, the different activities involved in data governance for the digital era tend to work from fundamentally diverging assumptions, which, when enmeshed in practice, are not immediately reconcilable. Competing concerns for data use cannot be resolved in advance through standardized resolutions, but require situated negotiations in the specific contexts, where tensions emerge. Existing data governance literature offers no basis for understanding or explaining how organizations can manage these complex, ill-structured problem domains (Simon 1973) unfolding across deliberate and emergent organizing of data-related activities in situated practice. To shed light on how organizations can cope, this dissertation builds on the notion of *data ventures* as an intellectual vehicle for examining the self-rising, organizational arenas, in which multiple managerial, operational, social and digital practices are enmeshed to devise appropriate data governance arrangements.

Empirical analysis of the evolving polycentric organizing logic in Fairview municipality shows that data ventures offer potent explanatory power as emergent collective-choice arenas, where operational rules governing everyday data use can be shaped by the practitioners, who are affected by them. As the four episodes progress, three data ventures are brought into being to resolve complex data governance issues, involving several individuals with diverging interests and perspectives on the situation. Each data venture co-evolves with the problematic situation across existing functions, roles, responsibilities and even organizational boundaries, and makes visible the situated interweaving of various data governance activities.

6.2.1. INTERWEAVING STRATEGIC AND OPERATIONAL ACTIVITIES IN PRACTICE

The data ventures reported in the Fairview case specifically demonstrate how appropriate data governance arrangements cannot meaningfully be devised at an abstract, strategic level, because data obtain their role as assets, when they are appropriated in specific, situated work practices.

In episode #2, the first data venture unfolds as citizens, public authorities and multiple local practitioners in Fairview butt heads about an existing data sharing practice in Technical and Environmental Services (section 5.3.3). As the Data Protection Agency had ruled, the procedure for publishing personal citizen data in public hearings was not governed by any legal basis in GDPR, which essentially meant these data were not by default assigned as assets to be governed. Yet, as the relative importance of personal data in the surrounding organizational environment had rapidly changed, they had now become valuable assets to certain citizens, who demanded they be governed as such. Multiple complaints and intense scrutiny contributed to growing tensions for practitioners in Technical and Environmental Services, who eventually decided to devise a working solution satisfying stakeholders. The Information security coordinator had limited insights into the work practices of the department and could not have anticipated the issue, while the IT and Digitalization department lacked appreciation for the working

context and could not independently develop a technical solution. Ultimately, tensions were effectively resolved in an emergent, situated collective-choice arena, where affected practitioners could shape new operational rules in the form of a PDF cleansing tool.

Likewise, in episode #3, a data venture is brought into being to allow the Information security coordinator to devise a multilateral data governance arrangement specifying how practitioners in Fairview can process and share sensitive, personal data in Outlook calendar entries. Despite leveraging numerous inputs from practitioners in various different departments and shaping an actionable, organization-wide guideline with many practical examples, individual departments are still confused about how to enact the rule in their own situated work practices. In episode #4, the coordinator is invited to give multiple presentations about the guideline in different departments, essentially demonstrating that data processing in calendar entries is inevitably intwined with situated work practices. In effect, however instrumental the guideline was, it still needed to be negotiated with affected practitioners in emergent collective-choice arenas to result in congruent operational rules. By the end, the formal outcome of the data venture constituted the general guideline for data processing in Outlook calendar entries, but in practice, multiple, informal adaptions had transpired and transformed the general arrangement into working operational rules.

To some extent, this data venture also exemplifies some characteristically problematic dynamics in separating activities of rule design and implementation in data governance (Alhassan et al. 2018). In episode #3, the Information security coordinator directs substantial resources toward conceiving just the right level of detail for an organization-wide arrangement that essentially intersects embodied individual habits for using Outlook as a coordination tool, situated work practices determining which data are assets and implicit, general assumptions about how to get travel reimbursements. Initially, the coordinator approaches the situation in a traditional manner; shaping the rule, getting support from top management and communicating to the organization, but it quickly unravels, as responses from practitioners indicate adopting the rule will not be straightforward. Eventually, the coordinator's presentation in different departments involve an interwoven cycle of design and implement activity, as practitioners reconceptualize the general arrangements into their own local environments, by asking domain contextual questions and the coordinator responds with an appropriate compromise.

6.2.2. PROGRESSIVELY TRANSFORMING EXISTING STATUS QUOS

Separating design and implementation activities implicitly also denotes a problematic separation between sustaining and mobilizing collective participation in data governance. As noted earlier (see section 3.2.2), supplying new institutions – sets of rules across operational, collective-choice and constitutional levels – for data governance in one major, transformational step by defining overall, abstract rules for organizing data (Khatri and Brown 2010) and systematically rolling them out (Ladley 2012) do little to incentivize

and mobilize participation. In polycentric governance, mobilizing and sustaining collective action are not seen as fundamentally different problems, but essentially as the continuous re-incentivizing of individual-level actions towards adopting coordinated strategies (Ostrom 1990). In practice, this means addressing smaller parts of a large-scale problem, with local, low-cost resolutions that demonstrate early success and high benefits to individuals (Ostrom 1990, p. 141). Rather than immediately devising complex, large-scale governance arrangements, each little change alters the overall structure of incentives; it is not about beginning from scratch, or taking one large transformational step, but about progressively transforming existing status quos (Ostrom 1990, 2005).

Emerging tensions between new data governance arrangements and latent status quos also come to expression through the data ventures reported in the Fairview case. First, in episode #2 as the data venture in Technical and Environmental services unfolds, practitioners initially resist adapting their data sharing procedure because it is deeply embedded in an existing work practice. Handling building permits was governed by multiple operational rules within the domain which had carefully been evolved in response to little incremental changes in the process over time. Although GDPR brought unprecedented attention to personal data for citizens, such data had been treated in the department for many years. Restricting access to data therefore involved changing a deeply established status quo, which was brought to the forefront in the data venture, where appropriate compromise was brokered.

Similar issues emerge in the data venture in episode #3, where the Information security coordinator addresses competing concerns for data in calendar entries to legitimate travel reimbursement requests. Despite general awareness that Outlook is unencrypted and the GDPR imposes hard sanctions on illicit sharing, practitioners remain convinced the Ministry of Finance has decreed the practice. Achieving the actionable Outlook guideline was challenging in itself, but the coordinator inevitably needed to address a second-order problem, which involved changing operational rules related to an existing, deep rooted assumption. In the data venture, tensions between new and existing practices were brought to the forefront and resolved, among other things by including a note about travel reimbursements in the final Outlook guideline (see section 5.4.2). Data ventures can bring attention to the unexpected or invisible status quos shaping current operational rules resulting in tensions as new data governance arrangements are devised.

6.2.3. NEGOTIATING INHERENT TENSIONS THROUGH RELATIONAL ETHICS

Beside illustrating and overcoming tensions between strategic design activities and operational implementation practices, the Fairview case also demonstrates how data ventures can evolve and be brought into being to negotiate inherent tensions arising in situations that involve sensitive and subjective data use. By the end of episode #4, the Information security coordinator indicates devising data governance will likely only grow more complex in the future, as datafication expands what can be known about social life.

Governance is no longer limited to discrete data sets, such as addresses, phone numbers and e-mails, but increasingly encompass sensitive, subjective conditions, like mental health, personality traits, life satisfaction, or political views as demonstrated in the Cambridge Analytica scandal (see section 1.2). While GDPR essentially offers a substitute ethical 'check-list', it is only appropriate for structuring formal litigation on what can and cannot be done, and as demonstrated in the Fairview case, cannot directly guide practices for responsive data use (Knox and Nafus 2018). As data ethics evolves as a contemporary discipline, organizations are increasingly encouraged to let go of the idea that ethics can be preprogrammed in universal rules and instead how ethical data processing can be negotiated through relationships of mutual respect and engagement on specific issues (Zigon 2019).

In the second data venture of episode #3, social workers look for an alternative solution for foster parents to provide their mandated status updates. This data venture is deliberately brought into being by the social workers themselves, as they know the information shared in these updates are sensitive and current practice involves the inappropriate exchange of Word-documents through proprietary e-mail clients such as Outlook (see section 5.4.3), which is not GDPR compliant. While both the Information security coordinator, the Digitalization director and an IT developer participate in the venture, the social workers' deep appreciation for the sensibilities and IT maturity of the foster parents determine which new data governance arrangements are considered appropriate. Rather than aiming for baseline compliance, for example through the standard online form, where data can be securely submitted, the social workers re-envision communication practices between foster parents, social workers and family care consultants. Eventually, the data venture resulted in a data governance arrangement dedicated to cultivating closer interpersonal relationships with foster parents and facilitating easier communication of sensitive subjects across municipal organizational boundaries, supported by an encrypted messaging service for mobile devices.

Similar tensions also became latent at the end of episode #4, where competing concerns for risk-scoring vulnerable, unemployed citizens materialized as the early indication of a data venture. Defining in legal terms why processing sensitive data on these citizens was necessary in a competence center could not be derived from formal regulations, while it was unclear how social workers decided whom to evaluate with the tool and how subjective characteristics were measured. In practice, the tool was developed to perform a critical service to protect employees in the competence center and help them take necessary precautions, when encountering citizens with a history of violence or crime (see section 5.4.3). By understanding the inherent ambiguities and complexities involved in processing subjective, sensitive data through a data venture, the heterogenous interests, concerns and perspectives of individual participants can be brought to the forefront, without being immediately settle in a legal framework. The Information security coordinator had great sympathy for both sides of the issue, even if the process by which these data were appropriated could not be sanctioned legally or formally. Although she ultimately concluded the tensions were inherently irresolvable and escalated the issue to

the DPO, she produced extensive documentation, detailing both the risks, impact and benefits of the solution for all affected participants.

In this vein, observations across the Fairview case also demonstrate how data ventures allow diverse heterogenous individuals, with otherwise conflicting interests, professional identities, norms and values to mutually accommodate and develop resolutions with the broadest possible coalition. In episode #2, practitioners in Technical and Environmental services did not strictly have to invest resources in changing their procedure, but ended up doing so anyway, which provided value to citizens. In episode #3, the social workers did not have to change their communication practices but appreciated how it would be beneficial to foster parents. In episode #4, the Information security coordinator did not have to present the guidelines to individual departments but acknowledged how it would be valuable for practitioners to voice their concerns and make sure they knew exactly how to remain compliant. Self-rising data ventures allow individuals to come together to solve a problem of mutual interest in a collective-choice action arena. Subsequently, they have the opportunity to interact with each other in a setting, where otherwise formal roles and responsibilities are temporarily absolved and social ties, trust and reciprocity can be developed, even if only concerning a bounded subject. As demonstrated with the Outlook guideline; devising congruent rules is not necessarily about how concrete and actionable it is, but more so about the social processes of interaction involved in addressing tensions, deliberating local conditions and experimenting with solutions.

6.2.4. ENMESHING DIGITAL AND SOCIAL PRACTICES

As data ventures bring attention to the mutually evolving, social processes of strategizing, coordinating and interpreting data use in organizations, they also make visible how such processes inevitably interweave with digital practices for amending and producing material arrangements for data use. Extensive literature on data-centric technologies (see section 2.1) encourage organizations to adopt big data analytics, AI, and blockchain to transform their operations, and gain competitive advantage (Kiron 2017; Kiron et al. 2014; Ransbotham et al. 2016; Ransbotham and Kiron 2017) and advocate for complementary investments in data governance, master data management and data scientists to gain business value. Such ideas indicate data can create value through the technologies, as they are implemented in the organization. Evidence from the data ventures in the Fairview case, however, seem to demonstrate that data are also constructed as a collective resource in an organization through its appropriation in situated work practices, which then determine the related technological solutions.

Across the three data ventures in Fairview, practitioners amend and produce material arrangements of data (Dourish 2017; McKinney and Yoos 2010) in a wide variety of ways. In the two data ventures in episode #2 and episode #3, the main outcomes are technological solutions; a PDF cleansing tool based on machine intelligence, which redacts data of specific format before displaying it in the archive, and a secure mobile, communication platform, which facilitates secure exchange of sensitive data across

organizational boundaries. Even the Outlook guideline, which as the outcome of its related data venture was purely behavior-based, still affected material arrangements of data, for example by limiting what data could be obtained from meeting screens and in open calendars. In all cases, the material arrangements of data were shaped by the mutually unfolding social processes and, because they were formed in a collective-choice arena, much more congruent with local conditions, than any standardized technological solutions. Consequently, practitioners were able to relate to data as a collective resource, because it was co-constructed within a bounded, organizational setting that made sense to them, as remarked by the business developer working with RPA in episode #4.

As part of an organizing logic for data governance in the digital era, data ventures bring attention to the situated interweaving of multiple strategic, managerial, operational, social and digital activities, as they unfold and at times conflict in practice. As emergent collective-choice arenas, data ventures enable otherwise heterogenous practitioners to cope with complex, ill-structured problems arising from tensions in practice and devise appropriate operational rules for data use in response. Data ventures remain distinct from other organizational forms, such as experiments and projects (Girard and Stark 2002; Kellogg et al. 2006), because roles and organizing are neither fixed nor anchored in hierarchy but allowed to co-evolve spontaneously around the emerging problem at hand with emphasis on mutual accommodation and norms of reciprocity. Data ventures bring attention to data governance as more than just design and implementation activities or formal outcomes, like principles, rules, roles, responsibilities and guidelines; they demonstrate data governance as emergent organizing of data use in everyday activities.

Neglecting the influence, power and potential of what occurs within these self-rising, temporary, situated action arenas is at best to discount a majority of the activity involved in governing data as a collective organizational resource, but at worst may impede further problem solving or value creation with data use in practice. As recounted by Ostrom:

> "we need to recognize that governance is frequently an adaptive process involving multiple actors at diverse levels. Such systems look terribly messy and hard to understand. The scholars' love of tidiness needs to be resisted. Instead, we need to develop better theories of complex adaptive systems focused on overcoming social dilemmas" (Ostrom 2005, p. 286)

Data ventures allow activities unfolding within emergent, spontaneous organizing to serve as productive, meaningful and valuable elements of data governance; not just appear messy, ad hoc, conflict-laden or problematic.

In extension of the pragmatist approach to qualitative case study work adopted in this dissertation (see section 4.1.2), data ventures should not be considered 'real' phenomena existing out there in organizational realities. Individuals essentially 'do' governance in data ventures; they respond to threats by considering, deliberating and experimenting with strategies for changing operational rules to best resolve issues. The role of knowledge in pragmatism is to be useful for action (Goldkuhl 2012), and thus data ventures offer an

intellectual vehicle for understanding and explaining how individuals in organizations can engage data governance through a constantly changing set of digital practices involved in organizing data use. Approaching data governance only as the act of supplying a new set of rules for how to treat data (as an asset by default) through chronological design and implementation activities neglects how data is spontaneously and continuously co-constituted as a resource in situated, work practices. Practical implications are discussed in the later section 6.5.

6.3. ORGANIZING PATTERNS OF POLYCENTRIC GOVERNANCE

Unlike open-access commons, traditional organizations can rely on formal hierarchy and authority to install behavioral and outcome controls that impose governance (Child and Rodrigues 2003). Such mechanisms are predominant in existing data governance research (Abraham et al. 2019) but limited in apprehending the multitude of operational activities involved in organizing data (Benfeldt et al. 2020; Parmiggiani and Grisot 2020), including those within spontaneously unfolding data ventures. Enforcing top-down control is likely to alienate practitioners (Constantinides and Barrett 2015) or result in conflicts or break downs in everyday governance practices (Boonstra et al. 2017) for data as a collective resource, even within organizational boundaries.

Arranging for the provision of data as a collective resource within an organization thus involves incentivizing a group of individuals with heterogenous interests and perspectives to adopt coordinating strategies for how they appropriate data in their local work practices. Individual departments depend on, produce and process data in multiple, overlapping ways to oversee their day-to-day responsibilities and may not voluntarily abide by general arrangements for data governance imposed by management. As detailed in the previous section on data ventures, congruent operational rules may readily be crafted in collective-choice arenas, where practitioners affected by the rules can participate in their making. An organizing logic of polycentricity can allow just enough situated, bounded autonomy within an overarching set of rules to negotiate congruent operational rules for local conditions, without descending into complete anarchy or destabilizing the entire system (Ostrom 1990, 2005).

Ostrom originally remarked that by polycentric principles she meant ”an essential element or condition that helps to account for the success of … institutions in sustaining the [natural resource systems]” (Ostrom 1990, p. 90). Subsequent research has found polycentricity to be an abstract notion for describing existing governance arrangements, which may manifest in the rules, boundaries and infrastructure of a system (Aligica and Tarko 2012; Carlisle and Gruby 2017; Mindel et al. 2018). Mindel et al. (2018) consolidates Ostrom’s eight principles to propose information commons may integrate polycentric governance into its design through four practices of boundary regulation, incremental adaption, shared accountability and provider recognition. As noted earlier (see section 3.3), information commons differ from data governance in that the former are concerned with open-access and free-riding problems but converge on similar concerns for mobilizing a group of heterogenous individuals to adopt coordinated strategies for governing a collective resource. As such, some overlap is inevitable with the organizing patterns described below.

Before Ostrom (1990) conducted her substantial empirical and theoretical work on the long-term sustainability of self-organizing resource systems, her husband Vincent Ostrom and colleagues characterized some systems underlying the organization of delivery of public services in U.S metropolitan areas as “polycentric political systems”

(Ostrom et al. 1961; V. Ostrom 1972). V. Ostrom argued that what looked like fragmented, overlapping, failing jurisdictions were in fact evidence of a new type of polycentric governance system, where "patterns of organization … will be self-generating or self-organizing in the sense that individuals will have incentives to create or institute appropriate patterns of ordered relationships" (1972, pp. 7–8). Thus, drawing on E. Ostrom's original eight principles, this dissertation sketches five organizing patterns of polycentric governance which are progressively enacted to facilitate both deliberate and emergent data governance activities within the empirical Fairview case. Table 11 roughly summarizes how the original principles inform the organizing patterns.

These organizing patterns can be perceived as component organizing logics of polycentricity, observed as loosely related structures of actions and activities initiated by practitioners in Fairview that are both enacted within data ventures and across the organization. By enacting five organizing patterns of boundary orchestration, situated resolution, distributed accountability, mutual accommodation and nested self-organizing, focal actors in Fairview engage both deliberate and emergent data governance activities to devise appropriate operational rules in response to competing concerns for data use. Table 12 at the end of this section summarizes how organizing patterns are enacted within data ventures and across the organization.

6.3.1. BOUNDARY ORCHESTRATION

Boundary orchestration involves activities, where practitioners actively determine which data are to be governed or treated as collective resources, how they are defined as such and most importantly; who are allowed to access, curate and share these data. In established data governance approaches, assigning decision-making rights and ownership of data assets are fundamental activities (Brous et al. 2016; Otto 2011b; Vilminko-Heikkinen and Pekkola 2019; Weber et al. 2009), but data are determined as assets at strategic level, based on overarching uses for the business (Khatri and Brown 2010). In the Fairview case, boundary orchestration activities seek to sketch overall parameters of a common data resource system at a high level of abstraction, and then progressively define individual responsibilities, as problems arise in practice. Effectively, boundary orchestration is enacted both deliberately, at organizational level, in work to map all IT systems, produce data processing agreements and prepare for formal auditing (episodes #1, #2), and emergently, within data ventures (episodes #2, #3) and other collective choice arenas (episode #4) as tensions or looming infractions require new rights for data curation, access, processing and sharing and thus corresponding reorchestration of the boundaries in the underlying resource system.

In episode #1, boundary orchestration is mainly accomplished by the then-IT manager looking to construct a shared IT architectural infrastructure. These ideas resonate with an established area of research on master data management, where data governance is seen as the overarching approach for coordinating ownership and accountability. At this point in Fairview, data governance is viewed as means for achieving coherence in IT

architecture, not for arranging provision of data as a collective resource and the IT manager and Digitalization director jointly devise a series of IT architecture principles (see section 4.2.3), indirectly sketching the boundaries for a common data resource system. One principle effectively shapes the future structure of incentives, namely by demanding that local system owners enter key information about their IT systems in the common coordination tool, Kitos. Unlike master data management, no standards are imposed for how the actual data models can look within each IT system, which upholds the Fairview tradition for local autonomy in IT acquisition, but only specifies a series of metadata about each IT system, which must be entered in standardized format. Ultimately, the overview in Kitos provides a virtualized version of the early boundaries for a common data resource system in Fairview, but without requiring the technological hassle often associated with establishing master data management (Vilminko-Heikkinen et al. 2016b; Vilminko-Heikkinen and Pekkola 2012, 2017), data warehouses (Alhassan et al. 2016) or data lakes (Porter and Heppelmann 2015).

As noted by Ostrom (1990), mere technical definition of boundaries is not sufficient, as they are meant to signify to individuals in the resource system who is in and who is out; whom to trust and form norms of reciprocity with. This level of orchestration becomes particularly important, if the resource is intangible and thus cannot be physically chalked up (Hess and Ostrom 2007). Boundary orchestration activities are therefore extended by the Digitalization director in episode #2, when he uses the Kitos overview to also register data processing agreements and auditor statements for IT systems. For IT systems, data processing agreements specify which data are processed in the system, how and by which individuals within the organization and under what legal purview this processing is done. Implicitly, such an agreement goes a long way to specify well-understood attributes of group members and what their mutual responsibilities are for given data resources (Ostrom 2005). As result, practitioners maintaining system entries in Kitos effectively orchestrates technical, organizational and social boundaries of the resource system.

Specific reorchestrations of these boundaries are also enacted within data ventures. During the second data venture in episode #3, the coordinator attempts to define certain meeting types to reorchestrate the boundaries for specific data resources, thus specifying how they may be processed and by whom. This is continuous, ongoing, extensive work, where the Information security coordinator experiences great difficulty in 'drawing the right lines' (see section 5.4.2.1). These difficulties persist into episode #4, where the coordinator has to continuously renegotiate for the data access rights to be upheld under specific, local conditions; she essentially has to reorchestrate boundaries once again during her presentation for Department of Children and Youth, where existing boundaries sketching internal unit confidentiality no longer apply (see section 5.5.1.1). These activities correspond with recommendations by Levitan and Redman (1998), who suggest it can be tempting to incorporate all accountabilities into one overall framework, but that "the policy should evolve as individual prescriptions are implemented" (p. 100).

Organizing patterns of polycentric governance		Ostrom's design principles (1990)
Boundary orchestration	Practitioners continuously arrange provision of data as collective resources by determining which data sets are involved, who in the organization (or outside) are allowed to curate, process or share them and how these rights may be coordinated	1. Clearly defined boundaries
Situated resolution	Operational rules governing data curation, processing or sharing are devised in situated, collective-choice arenas, such as data ventures, where practitioners in organizational settings that are affected by the rules can participate in making them	2. Congruence between appropriation and provision rules and local conditions 3. Collective choice arrangements
Distributed accountability	Practitioners arrange intricate sets of monitoring and sanctioning practices, where individuals self-monitor compliance and self-report infractions, while large-scale supportive institutions provide order, settle escalated disputes and offer support	4. Monitoring 5. Graduated sanctions
Mutual accommodation	Practitioners resolve problems in collective-choice arenas, where social norms of reciprocity develop and individuals respect diverging interests and work to accommodate each other, rather than trying to push their own agenda	6. Conflict-resolution mechanisms
Nested self-organizing	Self-rising, small-scale arrangements are recognized as legitimate; groups of practitioners are afforded autonomy to devise operational rules for resolving specific competing concerns in practice, which are then shaped by and progressively layered within a general set of rules	7. Minimal recognition of rights to organize 8. For CPRs that are parts of larger systems: Nested enterprises

Table 11. Organizing patterns of polycentric governance

In the empirical analysis, boundary orchestration activities are not only directed between different practitioners and departments within Fairview, but also with individuals outside the official organizational boundaries. In episode #3, the third data venture involves redesigning data sharing practices between internal family care consultants and external foster parents. Boundary orchestration activities here involve redefining which data are considered collective resources (sensitive information about foster children), how they should be governed by operational rules for use (must be exchanged through encrypted channels) and reestablishing mutual expectations and benefits between individuals (from providing one-way status updates to facilitating mutually beneficial communication practices). A dedicated material arrangement, the SecureDialogue app (see section 5.4.3) is developed to support and enforce these newly orchestrated boundaries.

Outward boundary orchestration activities address growing concerns in data governance literature about how to establish and enforce roles, rights and responsibilities for data sets that are not governed within a single organization, but rather across organizations (Buffenoir and Bourdon 2013; Tiwana et al. 2010), industries (Winter et al. 2019; Winter and Davidson 2019b) and regional legislations (Addis and Kutar 2018; Farshid et al. 2019; Li et al. 2019). New pursuits in data philanthropy (George et al. 2019; Taddeo 2016) and data monetization business models (Najjar and Kettinger 2013; Wixom and Ross 2017) require intricate, cross-organizational data governance arrangements, which may be established and continuously readjusted through delicate boundary orchestration. Complexities in boundary orchestration will only grow, as data-intensive digital services, such as social media platforms cross national, regional and global boundaries. In the aftermath of the Cambridge Analytica scandal (see section 1.2), the documentary *The Great Hack* (Amer and Noujaim 2019) follows a college professor from New York seeking to raise a case against Facebook for failing to disclose which of his data they process, with the then-EU membered British legal system, since GDPR legislation on data privacy and rights is only applicable in Europe. His pursuits ultimately fail, as accountability for his personal data disappears between incompatible governance structures (Winter and Davidson 2017). Outward boundary orchestration activities direct specific attention to such competing concerns and propose early ideas for how to manage these and other emerging tensions.

To Ostrom, well-defined boundaries is an important design principle, since it enables participants to know who is included in a set of relationships and whom to cooperate with (Ostrom 2005, p. 261), while boundaries imposed by external authorities are unlikely to be recognized by individuals, especially if they themselves have develop intricate patterns for organizing this resource in the past. Boundary orchestration plays an important role in data ventures, as these collective-choice arenas negotiate rules for issues within specific operational situations, with a great deal of autonomy; actively bounding where their resolutions apply is therefore important. While Ostrom (1990) emphasizes 'definition' and Mindel et al. (2018) emphasized 'regulation', this dissertation deliberately emphasizes 'orchestration' of boundaries, since the activities involved in this organizing pattern involve mediating between multiple heterogenous individuals, engaging various

strategic, operational, technical and social parameters, continuously readjusting which data are considered resources or assets, as they are co-constructed within situated work practices, balancing data rights defined in both small and large-scale arrangements, as well as facilitating outward appropriation activities across and between other formally defined boundaries.

6.3.2. SITUATED RESOLUTION

Situated resolution involves leveraging dedicated collective-choice arenas such as data ventures, to devise operational rules for data curation, processing or sharing activities in specific practice, in response to competing concerns emerging from tensions. Practitioners embedded in the organizational setting or otherwise affected by the rules are actively participating in the shaping of them. Recent data governance research has begun to reject ideas of data as intrinsically valuable, instead paying attention to how data obtains its role as asset or resource through co-construction with situated work practices (Monteiro and Parmiggiani 2019; Parmiggiani and Grisot 2020). In the Fairview case, situated resolution activities explicitly unfold within dedicated data ventures (see section 6.3), where specific problems unfold and are resolved in tailored data governance arrangements, and implicitly, across the organization, as the GDPR implementation is continuously reinterpreted into actionable guidelines (episode #2, #3).

The first dedicated data venture is brought into being as an emergent collective-choice arena at the end of episode #2, where competing concerns between citizens' demand for data privacy conflict with local practitioners in Technical and Environment services refusing to design a whole new procedure. Problem-solving within this arena focuses determinately on the local conditions within the department (a complex procedure honed over many years) and the data that citizens want protected (address, phone number and e-mail) to eventually develop a PDF cleansing tool, which redacts just the required data, without demanding major process remodeling. Previous literature on organizational data use has highlighted the importance of readjusting existing organizational routines, such that individuals can access, utilize and transform data into insight through appropriate structures, procedures and roles with regard for security, privacy and ethics (Mikalef, Pappas, et al. 2020; Tallon et al. 2013). Large-scale restructuring projects, complex technology development and core process reengineering are costly, risky and unlikely to succeed (Gust et al. 2017). Organizing patterns of situated resolution instead facilitate small-scale technical solutions, tentative process designs, and experimental cross-functional collaboration in multiple situated, data ventures.

A key feature of enacting situated resolutions across the organization is the opportunity to leverage shared norms, social ties, trust and reciprocity as otherwise heterogenous practitioners, with different ideological positions and interests are brought together in collective-choice arenas to address a problem of mutual interest. Instead of focusing on universal differences, the situatedness of a problem subtracts 'noise' from otherwise fundamental differences and allow practitioners to focus on problem deliberation,

bringing forth contextual expertise and experimenting with different solutions. In the Fairview case, this was particularly apparent in episode #2, where the Information security coordinator started experimenting with strategies for devising data governance, initially to remain GDPR compliant. She acknowledged that operational rules could not meaningfully be brought into action, if they were only communicated via e-mail; she had to show up, spend time with practitioners in their local context and listen to and understand their specific concerns, even if it meant they would ultimately end up doing the 'same' as other departments (section 5.3.2.1).

Empirical studies indicate data governance as a normative, organization-wide approach meets resistance in local practice, because overarching rules do not obviously translate to everyday activities (Begg and Caira 2011; Vilminko-Heikkinen et al. 2016a; Vilminko-Heikkinen and Pekkola 2019) and organizational practitioners tend not to commit beyond their own group-specific functions (Vilminko-Heikkinen and Pekkola 2019). Situated resolution activities do not presume practitioners can figure out for themselves how to appropriately translate general, organization-wide arrangements, but instead focus on how to mediate actionable changes with them in their situated work practices. Enacting this organizing pattern can consequently overcome some of the resistance likely to be met, as practitioners suddenly have to adapt carefully honed routines, without understanding why. In episode #4 of the Fairview case, the Information security coordinator persistently hosts the exact same presentation about the Outlook calendar guideline for multiple departments (section 5.5.1.1). When the Department of Children and Youth's management group requested the presentation be held once again, with a new selection of practitioners, it was evident that no matter how instrumental the guideline was, it still required situated negotiation with affected practitioners.

Processes for crafting rules are complex, but more likely to be effective, if they reflect existing relationships, norms and values with individuals (Ostrom 2005, p. 264) and local experimentation and resilience remain successful because "individuals who directly interact … with the physical world can modify the rules over time so as to better fit them to the specific characteristics of their setting" (Ostrom 1990, p. 93). Situated resolution activities address ongoing concerns in data governance about how strategic and managerial imperatives for data governance are consequently enacted and reshaped in everyday, situated work practices (Monteiro and Parmiggiani 2019; Parmiggiani and Grisot 2020), as social and digital practices enmesh. As data obtains its role as collective resource, when appropriated in situated work practices, enacting this organizing pattern can contribute to devising data governance arrangements that remain appropriate under specific local conditions.

6.3.3. DISTRIBUTED ACCOUNTABILITY

Distributed accountability involves arranging intricate sets of monitoring and sanctioning practices are distributed among internal groups and external institutions who offer support or settle escalated conflicts, while individuals self-monitor compliance and self-

report infractions. Recent concerns for data governance in practice involve growing frustrations that individual data sets are unlawfully repurposed or redistributed without knowledge or consent from the data subject (Cadwalladr 2019) while literature tends to focus on how to increase compliance, transparency and accountability in administration by specifying formal rules for data use (Breaux and Alspaugh 2011; Dawes 2010; Thompson et al. 2015). In the Fairview case, organizing patterns for distributed accountability do not depend on a single, central authority to know and enforce rules, but rather distributes monitoring, sanctioning and conflict resolution practices vertically and horizontally, within and outside the organization.

As episode #2 progresses, the Information security coordinator successfully enacts distributed accountability across the organization in multiple ways. Early attempts were made by the then-IT manager in episode #1, to impose certain IT architecture principles, which would restrict certain design choices and gradually demand conformance from local contractors. By contrast, the Information security coordinator had been hired to oversee day-to-day monitoring of GDPR compliance as Fairview had chosen the external DPO model. Subsequently, the coordinator managed to officially establish herself as a trustworthy, but official monitor among practitioners in Fairview. In episode #2, this is reflected in the way individuals frequently directs questions or concerns about their own working habits to the coordinator, who has invested heavily in engaging practitioners in the context of their organizational environments to build rapport (section 5.3.2.2). As practitioners continuously interact with the Information security coordinator to self-report infractions, she accumulates a backlog of most asked questions or reported violations, which in turn provides valuable information about where to direct her efforts.

As later remarked by Ostrom (2005), few self-organizing resource systems rely only on small-scale, bottom-up arrangements; they need complementary large-scale supportive institutions which can offer support and settle escalated disputes (p. 279). In Fairview, monitoring, sanctioning and conflict resolution practices are distributed among and supported in a web of different internal groups and external structures, each providing some form of authoritative legitimacy. In episode #3, the Information security committee, anchored at top management level, approve the final Outlook guideline (section 5.4.2.2), providing it with some legitimacy. Externally, Fairview's citizens could – and did – report suspected infractions either to Fairview's own DPO or directly to the national Data Protection Agency. If the agency upheld a complaint, then Fairview could worst case be reported to the police. In episode #4, formal notice of upcoming audits likewise functioned as a way to indirectly motivate compliance.

In corresponding data governance literature, transparency and accountability are pursued through formal governance arrangements which can demonstrate compliance to outsiders upon request (Breaux and Alspaugh 2011). In the Fairview case, the intricate arrangements established through distributed accountability activities are ultimately not for formal purposes, but to guide practice. In effect, monitoring and sanctioning practices were distributed at multiple levels of authority to motivate continued self-monitoring and

self-reporting in everyday activities; no practitioner wanted their department to be reported or found in violation, since this meant harsh sanctions, fines or heavy media attention (as was the case in section 5.3.3). Likewise, in episode #4, the Information security coordinator enacted distributed accountability, both through activities on legitimating system owner education as part of a formal audit (section 5.5.2), but also by escalating doubts about data processing in risk-scoring of unemployed citizens to the DPO (section 5.5.3).

Because there is no all-knowing, central authority to enforce agreements, polycentric arrangements require their own internal enforcements to ensure commitment and deter rule-breakers (Ostrom 1990). Enacting distributed accountability ensures that alternative monitoring, sanctioning and conflict resolution mechanisms exist to prevent infractions. Moreover, local practitioners are more likely to identify rule breakers long before any external monitors (Bennett et al. 2009), because they are actively involved in shaping rules and therefore motivated to monitor rule-breakers as a "by-product of their own motivations" (Ostrom 1990, p. 95) to engage in governance of the resource system. Since operational rules governing data use are often deeply contextual, and embedded in situated work practices, no one other than local practitioners can meaningfully know if infraction or violation has occurred. Enacting distributed accountability can disperse checks and balances for regulating the overall resource system across levels, to make it less prone to failure, since no single authority can effectively know or sanction everything at once, all the time.

6.3.4. MUTUAL ACCOMMODATION

Mutual accommodation involves devising operational rules in collective-choice arenas (as opposed to through general arrangements), such that otherwise heterogenous practitioners can establish social ties and norms of reciprocity around a problem of mutual interest and work to accommodate their individual interests, rather than push their own agenda. As datafication expands what can be known about social life (Lycett 2013; Sadowski 2019), data governance will increasingly have to address sensitive, subjective concerns (Knox and Nafus 2018). Current data governance approaches attend to such issues mostly through 'check-list' ethics (Janssen et al. 2020), but organizations are increasingly encouraged to let go of the idea that responsible data use can be preprogrammed in universal rules (Zigon 2019). In the Fairview case, mutual accommodation is enacted both explicitly in the individual data ventures but also implicitly across the organization as a whole to attend to complex, social dilemmas.

In episode #1, the then-IT manager acknowledged that enforcing top-down rules would never work in Fairview, due to its history and tradition for self-governance and local autonomy and the IT and Digitalization department is used to leveraging social capital, and offering assistance, rather than imposing rules. In episode #3, as the Information security coordinator seeks to mobilize collective participation for GDPR-related governance arrangements, she explicates that to her, data governance is a way of thinking,

which involves abandoning certain intuitive work practices for the sake of protecting data subjects' right to privacy (section 5.4.3). By extension, mutual accommodation activities expressly focus on downplaying universal judgments or preconceived notions, and instead seek new common ground as "stereotypes and evaluations are not fixed apart from the relationships and social contexts in which they develop [and] any collective actions that change relationships and contexts will affect beliefs, evaluations, and feelings" (Williams 1977, p. 375). Thus, most of the work to devise data governance in episode #3, both by the coordinator and the Digitalization director focuses on conveying GDPR as a new frontier in local government, to highlight positive assumptions of responsibility and ethics to practitioners, instead of compliance and harsh sanctions.

Organizing patterns of mutual accommodation are also enacted more broadly outside GDPR. In episode #4, this is particularly explicit, as the Business developer from IT and Digitalization recounts how establishing relations with local practitioners when developing RPA solutions are fundamental. He stresses that when initiating a project, he invests a great amount of resources in making individuals understand that the robot will not replace them or result in them being let go, but are there to help alleviate the work load, by eliminating menial data processing tasks and freeing up time for creative, problem-solving assignments (section 5.5.2). Similar actions occur in episode #3, where social workers remain acutely attentive to the situations of foster care parents, in re-envisioning their communication practices (section 5.4.3). Rather than thinking of all the infractions foster parents could potentially commit, they focus on use scenarios and the opportunity to improve the quality of communication between the family care consultants and foster parents.

Mutual accommodation is also enacted by the end of episode #4, where the Information security coordinator is tasked with handling the delicate issue of risk-scoring unemployed citizens with a history of crime and violence in Fairview's Competency Center. The Information security coordinator explicitly acknowledges the complexity and sensitivity of the topic, expressing sympathy for both the social workers and the citizens in question, and ultimately escalates the issue with the DPO. Before doing so, she undertakes meticulous risk, impact and benefit assessments to examine how the risk-scoring algorithm both positively and negatively affects individual parties. Officially, no legal basis exists for sanctioning the specific instance of data processing, but the coordinator nonetheless tries to emphatically reconcile interests. Mutual accommodation activities in this instance essentially demonstrates a developing case of relational ethics, where resolution of competing concerns for data use are resolved in relationships of mutual respect and engagement (Zigon 2019).

Cheap, local mechanisms for discussing and resolving what constitutes rule-breaking or suboptimal rules are critical in self-organizing governance arrangements, when no formal hierarchy can settle disputes. If these mechanisms are well-known to be effective among individuals, the overall number of conflicts are likely to reduce, since parties are aware issues can be escalated if need be (Ostrom 2005, p. 268). Enacting mutual

accommodation ensures "the interests of [all] parties will be in view, not just those of one participant" (Williams 1977), which is important in self-rising, autonomous, organizing, where individuals may not seek to evolve rules democratically by default, but descend into local tyrannies or power elites (Ostrom 2005, p. 282). As ambiguities, equivocality and social, moral dilemmas come to characterize organizational data use in the digital era (see section 2.1), organizing patterns of mutual accommodation can facilitate relational ethics, where practitioners negotiate parameters for responsible behavior through mutual respect and engagement.

6.3.5. NESTED SELF-ORGANIZING

Nested self-organizing involves empowering smaller groups of practitioners to devise operational rules for resolving specific competing concerns rising from tensions within their own situated work practices, while progressively layering these arrangements within a general set of rules. Self-rising, small-scale arrangements are afforded autonomy and recognized as legitimate, but ultimately nested within a set of rules at a higher level. Traditional separations of rational design decisions and practical implementation activities are predominant in established data governance approaches (Alhassan et al. 2018, 2019), but also proven problematic, as mobilizing support for prescriptive arrangements is difficult (Benfeldt et al. 2020) and may lead to breakdowns in practice (Boonstra et al. 2017). In the Fairview case, patterns of nested self-organizing is enacted both within data ventures and across the organization, which ultimately blends bottom-up and top-down structures.

Nested self-organizing activities begin to develop in episode #1, when local system owners are first tasked with maintaining Kitos entries; they are utmost experts in IT systems, data governance arrangements and domain specific data use and thus entrusted with updating necessary information in the overview tool. While the tool specifies how entries are made on a detailed series of system attributes, it does not impose data models or IT architecture requirements within the individual IT systems, effectively reconciling autonomous IT acquisition with a data overview. As the Information security coordinator was later hired in episode #2, nested self-organizing activities facilitated the arranging of monitoring and sanctioning practices, where practitioners were encouraged to engage in self-monitoring compliance and self-reporting infractions, but also to direct questions to an official monitor (section 5.3.2).

How this organizing pattern evolved is particularly explicit in episode #4. At the beginning, the Information security coordinator perceived the unremitting situational negotiations as ad hoc, messy and unorganized (see section 5.5.2), while the lack of progression on large-scale initiatives and planned activities frustrated her. Urgent issues were inconveniently materializing and requiring her attention. Yet, as the episode progressed and distributed success from small-scale arrangements accumulated, the coordinator could no longer ignore the benefits associated with progressively addressing tensions in practice and ultimately shifted her attention from advancing general

arrangements, to prioritizing solutions to emerging problems. Findings indicate data governance is often perceived as tedious (Ransbotham et al. 2016) and difficult to justify investments in (Begg and Caira 2012), unless an organization has already suffered major data breach (DalleMule and Davenport 2017). Nested self-organizing activities contributes to accretion of institutional capital and enable practitioners working with data governance to achieve small-scale benefits, which accumulate and highlights the importance of continued investments in data governance.

Nesting self-organizing was actively leveraged across the organization by the end of episode #4, as the Information security coordinator was planning the formal audit with the DPO. She expressly intended to use the impending audit as legitimate motivation for empowering decentral system owners to devise operational rules for data use within their own municipal domains (section 5.5.2). Simultaneously, Kitos entries would function as the central hook for local rules, where arrangements could be monitored by the Information security coordinator or used to demonstrate compliance in a formal audit, effectively nesting arrangements in a higher level of rules. In episode #1, both the IT manager and the Digitalization director had expressed a desire to function as a central coordination hub for IT acquisition in Fairview (section 5.2), but in episode #4, the Information security coordinator instead focused on enabling system owners to take responsibility for devising and nesting appropriate data governance arrangements irrespective of the IT systems they were using.

While nested self-organizing is enacted within data ventures to enable practitioners to devise appropriate situated, small-scale arrangements, some outcomes are interestingly perceived to be useful beyond the local conditions for which they were devised. In episode #2, the PDF cleansing tool developed as an outcome of the first data venture caught the attention of other departments dealing with similar processes of making public hearings accessible. In episode #3, the SecureDialogue solution is not only developed and implemented to support communication practices between foster parents and family care consultants, but also adopted by the Competence Center and the Substance Abuse Rehabilitation Center. This organizing pattern seemingly not only allows situated rules to be nested vertically in existing decision-making structures, but also vertically, across similar local conditions. Previously, data-intensive projects have been observed to suffer from function creep, as more and more stakeholders grow interested in a solution during its development and add on functionalities (Aaen and Nielsen 2018). Situated resolution can allow new technological arrangements to develop 'in peace', where nested self-organizing can subsequently enable the outcome to provide value in other, similar conditions.

As noted, nesting is a key feature of robust governance, because it helps overcome the problems associated with relying only on large-scale or small-scale governance arrangements (Ostrom 1990, 2005). Nested self-organizing is prerequisite in polycentric governance of data ventures, because it enables both deliberate and emergent organizing of data use; social norms, trust, expectations of reciprocity and deep contextual

knowledge can only be leveraged to resolve tensions close to empirical settings on a small scale, while general, stable expectations of behavior, as well as scientific knowledge, technological advancements and official settlement of disputes require supportive, overarching large-scale institutions (Girard and Stark 2002; Kellogg et al. 2006; Neff and Stark 2004). Nesting self-organizing essentially enmeshes top-down and bottom-up organizing, such that activities unfold in layers and allow individuals enough autonomy to deal with spontaneous disturbances in the system, while still maintaining some structured order of relationships; it ensures work accomplished in collective-choice data ventures is recognized as legitimate by the rest of the organization, while enforcing enough structure to prevent the surrounding organizational hierarchy from completely unravelling with totally autonomous entities.

Organizing patterns	Within data ventures	Across the organization
Boundary orchestration	New curation, access, processing and sharing rights are determined for specific data in response to emerging problems with existing practice, and new memberships are established to determine who is allowed to appropriate data	Practitioners engage in various activities to map all IT systems, produce data processing agreements, prepare for formal auditing statements to continuously orchestrate boundaries of a common data resource system, despite fragmented IT architecture
Situated resolution	Operational rules for data use are negotiated with practitioners affected by the rules, close to the situated work practices where data curation, access, processing and sharing occurs	Organization-wide data governance arrangements are devised with input from practitioners and consequently renegotiated into specific operational rules within individual municipal domains
Distributed accountability	Practitioners are allowed to devise operational rules for a bounded area of the resource system, but are still accountable to and shaped by a general set of rules at a higher level	Monitoring and sanctioning practices are distributed among external institutions and internal groups, while individuals self-monitor compliance and self-report infractions to official monitors
Mutual accommodation	Problem-solving in collective-choice arenas allow practitioners to establish social ties and norms of reciprocity to mutually accommodate differences and seek solutions with broadest possible coalition	Abstract, general legislation is continuously translated and reinterpreted with practitioners in mind and voicing doubts or possible infractions are seen as positive and encouraged
Nested self-organizing	Negotiated operational rules, data governance arrangements and technical solutions are recognized as legitimate outcomes of collective-choice activity	Multiple local practitioners are empowered to devise small-scale arrangements for specific operational rules which are then complimented by large-scale supportive arrangements

Table 12. Organizing patterns within data ventures and across the organization

6.4. PRACTICAL IMPLICATIONS

Inherent features of polycentric governance and data ventures demonstrate that they are emergent phenomena, which unfold in response to specific fluctuations within a bounded resource system. Generalizing implications from the Fairview case as a blueprint for engaging polycentric organizing is not only unethical, but goes against the very nature of self-rising, adaptive institutions (Ostrom 2005). Yet, as this dissertation undertook an engaged scholarship approach in the form of a pragmatist-oriented case study, some modest coping methods for dealing with competing concerns for data use in the digital era are tentatively outlined in the rest of this section.

6.4.1. PROGRESSIVELY CHANGE STATUS QUOS RATHER THAN LOOK FOR THE SILVER BULLET

Much data governance literature has attempted to identify which set of contingent contextual factors facilitate and inhibit adoption of data governance (Begg and Caira 2012; Mikalef and Krogstie 2020; Weber et al. 2009), so as to incorporate them in the design. Empirical insights from the Fairview case however suggest searching for the silver bullet solution in the form of the right rules requires substantial resources and will still not immediately be adopted broadly in an organization, no matter how actionable it is. Rather than spending disproportionate time designing the right structures, practitioners looking to evolve data governance could instead focus on addressing the issues that are voiced by individuals in the organization, as they experience them in their situated work practices. A humble suggestion is to remain patient with (the lack of) progression of large-scale initiatives, and instead trust that multiple, local resolutions of emergent issues is not messy, ad hoc or a waste of time, but rather cheap, valuable investments in progressively changing the structure of incentives for adopting more broad or general data governance arrangements in the future.

6.4.2. COMBINE TOP-DOWN AND BOTTOM-UP INITIATIVES IN NESTED SELF-ORGANIZING

During the problem formulation study preceding the work in this dissertation, multiple Digitalization directors, IT managers and Digitalization consultants disclosed that devising rules for specific issues like metadata, data quality and data access seemed like an insurmountable task to undertake for an entire organization (Nielsen et al. 2018). Here, it should be reiterated that data curation, processing and sharing are activities inevitably co-constituted by situated, local work practices, as is demonstrated several times in the empirical case of Fairview. No IT and Digitalization department can be expected to imagine all the possible operational rules for governing specific data use that unfolds in highly specialized domain work. Instead, practitioners may find it useful to enact nested self-organizing, in a way that combines some loosely conceived, large-scale arrangements specifying concerns for data as a collective resource, with more local autonomy to actually devise operational rules. Focusing only on data governance within a limited team or work

process can allow individuals to cope with the complexity at hand, and not try to imagine how it must be in all other practices, even if successful arrangements may be scaled up, like the PDF cleansing tool in the Fairview case.

6.4.3. START SMALL AND ACKNOWLEDGE THE VALUE OF DATA IN SITUATED WORK PRACTICES

Empirical studies have repeatedly highlighted the difficulties that practitioners experience in trying to understand and communicate the value of data governance investments (Ladley 2012; Ransbotham et al. 2016; Vilminko-Heikkinen and Pekkola 2017). In some cases, only a breach or leak can justify such investments (DalleMule and Davenport 2017). In the Fairview case, insights suggest data tends to obtain its role as a collective resource to be governed, not by default, but when processed as part of a work arrangement in a specific context (like addresses in certain calendar invites). Organizations looking to get started with data governance or other data-centric technologies like blockchain or AI may find it useful to focus on how data obtains its role in very specific contexts or work and while it may seem unambitious when sidelined with ongoing innovations in Silicon Valley, it goes a long way in establishing the concept and potential of data as a collective resource. This is especially encouraged in organizations, where most data governance arrangements are managed or progressed by IT professionals, since they may take for granted the usefulness and potential of data-centric technologies.

6.4.4. LEVERAGE COLLECTIVE CHOICE WHEN IMPLEMENTING GENERAL ARRANGEMENTS

In the past, cybersecurity policies, standardized IT and to some extent GDPR legislation have been known to meet resistance in local work practices, when they are perceived as prescriptive, management controls imposed from above to make life miserable (Goodhue et al. 1988). In the Fairview case, multiple individuals express they do not want information security to be seen as a hurdle to be overcome. A modest suggestion is to actively leverage collective-choice arenas, either formal or informal to interweave managerial and operational choices and to sincerely engage in dialogue with practitioners about how general arrangements may be translated to local operational rules. The time and energy spent doing so may be considered as further investments in ensuring the already costly elaborate arrangements are also adhered to in practice.

6.4.5. ENGAGE MUTUAL ACCOMMODATION AS A FEATURE, NOT A HURDLE

Finally, attention to data subjects' rights have exploded in the aftermath of recent incidents (Gabrys 2019), like the Cambridge Analytica scandal and instatement of the GDPR. In turn, the relative importance of certain data as collective resources have changed rapidly, and it is unrealistic to expect organizations to have it all under control

at this point. Technological advances that expand what can be known about social life have come to stay, and data use is only likely to become more complex, sensitive and conflict-laden, as deeply subjective conditions, like mental health, personality traits, life satisfaction, political views and many more can be appropriated in algorithms. Drawing on extant literature and empirical insights, it is strongly encouraged that organizations pursue mutual accommodation and relational ethics as a feature, rather than a hurdle. Actively orchestrating the outward boundaries of their data resources and ensuring responsible, accountable data use will not only ensure formal compliance or avoid media scandals, but help even the playing field in a datafied society, where power, knowledge and skill are increasingly amassing within a small group of people, who truly know and understand what goes on inside an algorithm (Zuboff 2018).

CHAPTER 7. CONCLUSION

7.1. CONTRIBUTIONS

Detailed in Chapter 1, the primary objective in this dissertation was to advance knowledge on data governance by theorizing a corresponding organizing logic for the digital era. Drawing on Ostrom's (1990) characterization of robust, self-organizing resource systems to analyze material from a two-year case study, the dissertation sought to address the research question:

RQ: How does an organizing logic of polycentricity evolve and enable an organization to devise appropriate data governance arrangements in response to competing concerns for data use in the digital era?

Key insights from the empirical analysis were leveraged in combination with insights from extant literature to clarify how an organization could engage in deliberate and emergent organizing of data use through polycentric governance of organizational data ventures.

In response to the research question, an organizing logic of polycentricity explicates how data ventures unfolded and were brought into being as self-rising, organizational arenas, where individuals interwove multiple strategic, managerial, operational, social and digital practices to adapt operational rules for data use in response to competing concerns arising in practice; it also explicated how five polycentric organizing patterns of boundary orchestration, situated resolution, distributed accountability, mutual accommodation and nested self-organizing were progressively enacted, as loosely related structures of actions and activities, within data ventures and across the organization, to devise appropriate data governance arrangements. Examined in the context of a traditional, bureaucratic organization, this process involved mediating multiple, often diverging perspectives and interests of a wide range of heterogenous stakeholders within and across organizational levels and boundaries.

As the empirical foundation for its theorizing, the dissertation examined the case of Fairview municipality in which focal actors progressively enacted polycentric governance to form, adapt, and evolve various data governance arrangements and where multiple data ventures unfolded and were brought into being to resolve competing concerns for data, as they became salient in practice. The theoretical framing allowed the analysis to zoom in and out on organizational processes to capture the interweaving of managerial decisions about the overarching direction for data use with improvised operational choices for how to appropriate specific data sets under local conditions; it also illustrated

how social processes of strategizing, coordinating, communicating and interpreting in data-related activities were enmeshed with digital practices of producing and amending material arrangements of data.

Consequently, the work contained in this dissertation contributes primarily to data governance literature, summarized in Table 13 and detailed in the next subsection. While not directly the focus, the work contained in this dissertation also offer some tentative contributions to broader literature detailed in final section and summarized in Table 14.

7.1.1. CONTRIBUTIONS TO DATA GOVERNANCE RESEARCH

Scholars have recently begun to recognize the limitations of understanding data governance purely in terms of traditional approaches, like formal principles, structures, decision-making rights and asset management (Abraham et al. 2019). Understandings of how day-to-day decision-making unfolds in practice remain unexplored (Alhassan et al. 2016, 2018; Parmiggiani and Grisot 2020), which only becomes more problematic, as empirical studies find data governance is difficult in practice (Begg and Caira 2012; Nielsen et al. 2018), data does not immediately translate to assets for practitioners (Nielsen et al. 2018), and emerge only as such when appropriated in situated work practices (Monteiro and Parmiggiani 2019) and everyday data curation activities (Parmiggiani and Grisot 2020).

In this regard, a primary contribution in this dissertation is the conceptualization of data ventures. As part of an organizing logic for data governance in the digital era, data ventures bring attention to the situated interweaving of multiple strategic, managerial, operational, social and digital practices, as they unfold and at times conflict in practice. As emergent, but situated collective-choice arenas, data ventures enable practitioners to spontaneously cope with complex, ill-structured problems arising from tensions in practice and devise appropriate operational rules. Data ventures bring attention to data governance as more than just design and implementation activities or formal outcomes, like principles, rules, roles, responsibilities and guidelines as requested by literature; they demonstrate data governance as emergent organizing of data use in everyday activities.

Organizational data use is increasingly characterized by tensions (see Chapter 2), while fluctuating external and internal demands for data require responsive data governance (Tallon et al. 2013; Weber et al. 2009). Prior studies on data governance have predominantly adopted "one-off" or cross-sectional perspectives (Abraham et al. 2019, p. 433), while only a handful of studies reflect how isolated data governance concepts, such as strategy (Tallon et al. 2013) ownership (Vilminko-Heikkinen and Pekkola 2019) and effectiveness (Otto 2013) might need to change over time. The second major contribution of this dissertation is therefore the processual account of how an organizing logic for data governance progressively evolves, as practitioners enact a series of polycentric organizing patterns. The empirical analysis shows how the organization responds and adapts to rapid external change following from instatement of regional data

protection legislation by progressively enacting organizing patterns to devise appropriate data governance arrangements. Moreover, the discussion highlights how these structures of actions and activities are enacted both within data ventures and across the organization, contributing with a holistic perspective on how data governance evolves within an organization, rather than just isolated concepts.

Extant data governance literature has focused extensively on the implementation of formal rules and responsibilities, which specifies decision-making and accountabilities within a series of decision domains regarding an organization's data assets (Khatri and Brown 2010; Otto 2011c, 2011d). While previous work offer valuable insights, it still remains unclear how and when to adopt centralized, decentralized or hybrid designs (Abraham et al. 2019). As its third contribution, this dissertation suggests governance designs are not universal, but rather progressively formed and adapted through nested self-organizing activities, where top-down and bottom-up approaches can be combined and tailored to the specific conditions of the organization. Moreover, evidence from boundary orchestration activities suggests determining and distributing rights for data processing is likewise an evolving matter, where group memberships are continuously reorchestrated in response to emerging tensions in practice.

Researchers have started highlighting the potential of data governance for managing complex issues of privacy, data protection legislation and ethics in organizational data use (Abraham et al. 2019; Addis and Kutar 2018; Vydra and Klievink 2019). The fourth contribution of this dissertation lies in the detailed empirical account of how an organization evolves polycentric governance in response to rapid external change. This empirical account exemplify the increasingly complex issues related to devising data governance arrangements that support formal GDPR compliance, but also how appropriate operational rules for ethical data use may be crafted in sensitive contexts. While situated resolution and mutual accommodation activities offer insights into how specific arrangements can be devised responsively as tensions emerge in practice, nested self-organizing ensures that the local autonomy is subject to a broader set of rules, not only within organizational boundaries, but also in national courts and data protection agencies.

Growing concerns in data governance literature also direct attention to how organizations establish and enforce roles, rights and responsibilities for data sets that are not governed within a single organization, but rather across organizations (Buffenoir and Bourdon 2013; Tiwana et al. 2010), industries (Winter et al. 2019; Winter and Davidson 2019b) and regional legislations (Addis and Kutar 2018; Farshid et al. 2019; Li et al. 2019). New pursuits in data philanthropy (George et al. 2019; Taddeo 2016) and data monetization business models (Najjar and Kettinger 2013; Wixom and Ross 2017) require intricate, cross-organizational data governance arrangements. As a fifth contribution, the empirical account and theorizing of outward boundary orchestration activities may represent early attempts to propose how such arrangements may be established and continuously readjusted. Complexities in inter-organizational data

governance will only grow, as data-intensive digital services, such as social media platforms cross national, regional and global boundaries. Outward boundary orchestration activities propose early ideas for how to manage these and other emerging tensions that cross organizational boundaries.

A final contribution of the organizing logic for polycentric governance of data ventures to data governance literature is its attention to progressively mobilizing collective action for organization-wide data governance arrangements. Empirical studies find that mobilizing organizations to adhere to standardized data principles remains difficult (Nielsen et al. 2018), the value of data as an organizational asset is not immediately clear in practice (Vilminko-Heikkinen et al. 2016a) and organizational members tend not to commit beyond their own group-specific functions (Vilminko-Heikkinen and Pekkola 2019). The proposed organizing logic focuses on progressive evolution and emergent organizing, where data ventures unfold and can be brought into being as dedicated collective-choice arenas, where practitioners affected by operational rules also participate in crafting them. As such, small-scale arrangements demonstrate benefits to practitioners within their own local work environment and accumulate to mobilize collection action across the entire organization

Research area	Concern	Contribution of this dissertation
Data governance mechanisms	Limited attention is paid to how data governance activities unfold in everyday practices (Monteiro and Parmiggiani 2019; Parmiggiani and Grisot 2020)	Data ventures bring attention to how various strategic, managerial, operational, social and digital practices enmesh as data governance unfolds in practice
	Limited attention is paid to how data governance evolves over time (Abraham et al. 2019; Otto 2013; Tallon et al. 2013; Vilminko-Heikkinen and Pekkola 2019)	A longitudinal account of how data governance as an organization-wide approach evolves and adapts within an organization over time is presented
	Unclear under which circumstances centralized, decentralized and hybrid designs should be undertaken (Otto 2011c, 2011d; Weber et al. 2009)	Organizing patterns demonstrate effective governance designs are not universal, but progressively evolved through nested self-organizing where top-down and bottom up approaches can be tailored and combined
	Determining the right distribution of data ownership and accountability is difficult (Otto 2011c; Vilminko-Heikkinen and Pekkola 2019)	Rights and responsibilities for data as a collective resource are progressively determined as emerging tensions direct attention to the need for reorchestrating inward boundaries and establish new rights

	Concerns about how to enable data-centric innovation with simultaneous consideration of privacy and ethics (Abraham et al. 2019; Addis and Kutar 2018; Vydra and Klievink 2019).	Inherently competing concerns for data-centric innovation and data ethics may be contextually resolved through relational ethics enacted in mutual accommodation activities
Data governance scope	Little knowledge on how to govern data in inter-organizational relationships (Addis and Kutar 2018; Buffenoir and Bourdon 2013; Farshid et al. 2019; Li et al. 2019; Tiwana et al. 2010),	Organizing pattern of outward boundary orchestration offer preliminary insights into how inter-organizational governance arrangements may be formed and adapted
	Data are presumed to be assets by default (Monteiro and Parmiggiani 2019; Parmiggiani and Grisot 2020)	Data ventures demonstrate how the value of data as a collective resource is both co-constituted with situated work practices and generated as specific competing concerns result in salient tensions in practice
	Difficult to foster cross-organizational data sharing (Vilminko-Heikkinen et al. 2016b; Vilminko-Heikkinen and Pekkola 2017)	Cross-organizational collaboration may be fostered in emergent collective-choice arenas where practitioners can deepen social ties through problem-solving
Data governance contingency factors	Unclear what facilitates adoption of data governance and what inhibits adoption (Abraham et al. 2019; Begg and Caira 2011; Tallon et al. 2013; Weber et al. 2009)	Collective action for organization-wide data governance may be progressively achieved by transforming small-scale status quos
	Unclear which contextual factors need to be considered when designing data governance (Abraham et al. 2019; Begg and Caira 2011; Tallon et al. 2013; Weber et al. 2009)	Collective-choice arenas can allow congruent operational rules to be devised progressively with local conditions in mind, but also with adaption to fluctuations in surrounding environment

Table 13. Contributions to data governance literature

7.1.2. TENTATIVE CONTRIBUTIONS TO BROADER LITERATURE

This dissertation set out to advance knowledge on an organizing logic for data governance in the digital era, but ultimately touched upon multiple other streams of research and areas of concern in the literature. Some tentative peripheral contributions may be identified from the work to address emerging research concerns and potentially serve as suggestions for future research.

First, this dissertation adopted a broad understanding of data governance as the fast-growing, constantly changing set of digital practices involved in the organizing of data (see section 2.4). As noted in Chapter 1, data governance emerges as the foundation for pursuing nearly any other digital trend, such as blockchain, AI, and data analytics. While the organizing logic-framing proposed here served the specific purpose to examine data governance, it represents some early steps toward an integrative understanding of the mutual issues of governance, technology and organizing for data use; a topic which deserves broader attention from the IS community. Governing data in practice means interweaving managerial decisions about the overarching direction for data use with improvised operational choices for how to appropriate specific data sets, when performing work under local conditions, restraints and opportunities. It means enmeshing social processes of strategizing, coordinating, communicating and interpreting with numerous technical practices for producing and amending material arrangements of data. The IS research tradition is well-positioned to examine these dynamics.

Secondly, this dissertation observed how organizational data use in the digital era may be characterized by fundamentally competing assumptions of techno-optimism and techno-skepticism (section 2.1). Moreover, it has paid specific attention to how ethical concerns may be confronted, negotiated and resolved through situated resolution activities (section 6.3). As datafication expands what can be known about social life, 'check-list' ethics remain insufficient in guiding practices for data scientists, software developers and others developing data-centric technology (Knox and Nafus 2018). The empirical analysis in this dissertation has offered some preliminary insights into how relational ethics, where ideas about right and wrong are continuously renegotiated in relationships of mutual respect and engagement (Zigon 2019), can be organized and coordinated in practice. Future IS research should expand this purview and consider questions on how accountability, responsibility and transparency can be negotiated without restricting practitioners' work practices or data-centric technology innovation (Abraham et al. 2019).

Third, in the empirical analysis, specific data ventures brought into view how practitioners enmeshed social processes of strategizing, coordinating, communicating and interpreting in data-related activities with producing and amending material arrangements of data (section 6.2.4). Among multiple understandings of data, a token view asserts that information acquires tangibility when encoded and processed as data in information systems, where it can then be stored, shared, retrieved, manipulated and distributed (McKinney and Yoos 2010; Mindel et al. 2018). When a practitioner in an organization records enumerated data items in a spreadsheet, manipulates them through functions and formula, saves and forwards the file by e-mail to a colleague, they essentially engage in appropriation activities of a collective resource comparable to fishermen trawling fresh-water minnows in an inshore fishery. Despite general notions of data as abstract and intangible, such activities are nonetheless indications of how knowing becomes material in data ventures (Monteiro and Parmiggiani 2019).

Finally, this dissertation proposed the novel conceptualization of data ventures (section 2.3). Combined with the pragmatist approach to a qualitative, case study and an engaged scholarship approach, this dissertation engaged in blue ocean theorizing (Grover and Lyytinen 2015). While it also undertook careful empirical work to address the research question and explore concepts and ideas in an organizational setting, theorizing in this dissertation involved leveraging familiar physical or linguistic objects to highlight, clarify, enrich and enlighten meaning (Hassan et al. 2019) about a fast-growing, constantly changing set of digital practices. Theory development in this study was not primarily concerned with knowledge for explanation (as in positivist traditions) or understanding (as in interpretivist traditions), but knowledge, which was useful for action (as in pragmatist traditions). Even if data ventures are merely intellectual vehicles, it is the hope they will stipulate further dialogue by offering new concepts that are useful for researchers in coping with, reasoning about and further investigating the many, multidisciplinary issues implicated in the sociotechnical data phenomenon.

Literature	Concern	Tentative contribution
Information systems research	No converging body of IS literature addresses organizational data use	Proposition for advancing knowledge on the fast-growing, constantly changing set of digital practices involved in the organizing of data use in the digital era
	New approaches for organizational data resource management in the digital era (Levitan and Redman 1998)	A non-hierarchical organizing logic for data resource management in the digital era which still focuses on ownership and responsibility
	Concerns that techno-optimism is fundamentally incompatible with techno-skeptic concerns (Zuboff 2018)	An empirical account and subsequent theorizing of how responsibility, accountability, ethics and morality can be enacted in an organization through mutual accommodation and situated resolution
	Need for more insights on how knowing in information systems becomes material in practice (Monteiro and Parmiggiani 2019)	A detailed, processual, empirical account of how digital practices for data use unfolds through social processes and becomes material in data ventures
Methodologies for advancing IS theorizing	More attention is needed to how contemporary IS phenomena may be studied through discursive practices and unfettered blue ocean theorizing (Hassan et al. 2019; Grover and Lyytinen 2015)	Conceptualizing data ventures is an attempt at leveraging metaphorizing to produce enunciations and highlight meaning about a fast-growing, constantly changing set of contemporary digital practices (data governance) which receives little attention in established IS research
	Concerns about how to study consequences of datafication in society (Knox and Nafus 2018)	Engaged scholarship and a pragmatist-oriented case study bring attention to actions and activity unfolding in practice as a way to study data

Polycentric governance of resource systems	Original work focuses on solving problems of free-riding, openness and accessibility (Ostrom 1990; Mindel et al. 2018)	Extends the perspective to account for how polycentric governance of a collective resource also contribute to organizing within organizational boundaries
	Original work focused on natural physical resources, but research also calls for how to manage intangible resources (Ostrom 2005; Hess and Ostrom 2007)	Detailed empirical account on how to govern data as an intangible resource

Table 14. Tentative contributions to other areas in the literature

7.2. CONCLUDING SUMMARY

This dissertation proposed *data ventures* as an intellectual vehicle for explaining the self-rising, organizational arenas, in which individuals negotiate competing concerns for data use as they emerge in practice (Chapter 2). Drawing on foundational themes from research on polycentric governance in self-organizing resource systems (Chapter 3), this dissertation then undertook an empirical analysis of a two-year, qualitative, case study focusing data governance arrangements within Fairview, as they evolved before, during and after formal instatement of GDPR (Chapter 4). The empirical analysis provided a processual account of how tensions emerged, how dedicated data ventures unfolded and were brought into being to negotiate competing concerns and how appropriate data governance arrangements were devised in response (Chapter 5).

Empirical insights were leveraged in combination with extant literature to theorize polycentric governance of data ventures, which explicated how a polycentric organizing logic evolved and enabled Fairview to devise appropriate data governance arrangements (Chapter 6). Data ventures were brought into being as self-rising, situated, arena in which strategic, operational, social and digital practices were enmeshed to devise appropriate data governance arrangements (section 6.2), while five organizing patterns of polycentric governance were progressively enacted within data ventures and across the organization to facilitate deliberate and emergent organizing of data governance activities (section 6.3).

By introducing polycentric governance of data ventures as a novel theorization, this dissertation extended data governance research on traditional, hierarchical approaches. Data ventures bring attention to how data-related activities emerge, interweave and unfold in situated work practices, while polycentric governance contributed with a processual perspective on how data governance arrangements may be adapted and evolved progressively; over time, in response to rapid external change or emerging internal tensions; and outside organizational boundaries to orchestrate inter-organizational governance arrangements (section 7.1). Together, these insights contribute to broader IS literature by reestablishing data governance as a fast-growing, constantly changing set of digital practices involved in the organizing of data

REFERENCES

Aaen, J., and Nielsen, J. A. 2018. "The Dark Side of Successful Data Intensive Projects: Function Creep and Stakeholder Creep," in *Proceedings of the 26th European Conference on Information Systems*.

Abbasi, A., Sarker, S., and Chiang, R. 2016. "Big Data Research in Information Systems: Toward an Inclusive Research Agenda," *Journal of the Association for Information Systems* (17:2), I–XXXII.

Abraham, R., Schneider, J., and vom Brocke, J. 2019. "Data Governance: A Conceptual Framework, Structured Review, and Research Agenda," *International Journal of Information Management* (49), pp. 424–438.

Addis, M. C., and Kutar, M. 2018. "The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness," *UK Academy for Information Systems Conference Proceedings 2018* (29), p. 24.

Agarwal, R., and Dhar, V. 2014. "Editorial: Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research," *Information Systems Research* (25:3), pp. 443–448.

Agency for Digitisation. 2016. "A Stronger and More Secure Digital Denmark - The Digital Strategy 2016-2020,".

Alhassan, I., Sammon, D., and Daly, M. 2016. "Data Governance Activities: An Analysis of the Literature," *Journal of Decision Systems* (25:1), pp. 64–75.

Alhassan, I., Sammon, D., and Daly, M. 2018. "Data Governance Activities: A Comparison between Scientific and Practice-Oriented Literature," *Journal of Enterprise Information Management* (31:2), pp. 300–316.

Alhassan, I., Sammon, D., and Daly, M. 2019. "Critical Success Factors for Data Governance: A Theory Building Approach," *Information Systems Management* (36:2), pp. 98–110.

Aligica, P. D., and Tarko, V. 2012. "Polycentricity: From Polanyi to Ostrom, and Beyond," *Governance: An International Journal of Policy, Administration, and Institutions* (25:2), pp. 237–262.

Alofaysan, S., Alhaqbani, B., Alseghayyir, R., and Omar, M. 2014. "The Significance of Data Governance in Healthcare - A Case Study in a Tertiary Care Hospital:," in *Proceedings of the International Conference on Health Informatics*, pp. 178–187.

Al-Ruithe, M., and Benkhelifa, E. 2017. "A Conceptual Framework for Cloud Data Governance-Driven Decision Making," in *Conference Proceedings - 2017 International Conference on the Frontiers and Advances in Data Science, FADS 2017* (Vol. 2018-January), pp. 1–6..

Al-Ruithe, M., Benkhelifa, E., and Hameed, K. 2018. "A Systematic Literature Review of Data Governance and Cloud Data Governance," *Personal and Ubiquitous Computing*, pp. 1–21.

Amer, K., and Noujaim, J. 2019. *The Great Hack*, Documentary, Netflix.

Avison, D. E., Lau, F., Myers, M. D., and Nielsen, P. A. 1999. "Action Research," *Communications of the ACM* (42:1), ACM New York, NY, USA, pp. 94–97.

Baskerville, R. L., and Myers, M. D. 2002. "Information Systems as a Reference Discipline," *Mis Quarterly*, JSTOR, pp. 1–14.

Baskerville, R. L., and Myers, M. D. 2004. "Special Issue on Action Research in Information Systems: Making IS Research Relevant to Practice: Foreword," *MIS Quarterly* (28:3), pp. 329–335.

Begg, C., and Caira, T. 2011. "Data Governance in Practice:: The SME Quandary Reflections on the Reality of Data Governance in the Small to Medium Enterprise (SME) Sector," in *The European Conference on Information Systems Management*, , September, pp. 75–VIII.

Begg, C., and Caira, T. 2012. "Exploring the SME Quandary: Data Governance in Practise in the Small to Medium-Sized Enterprise Sector," *The Electronic Journal Information Systems Evaluation* (15:1), pp. 1–12.

Benbasat, I., Goldstein, D. K., and Mead, M. 1987. "The Case Research Strategy in Studies of Information Systems," *MIS Quarterly*, JSTOR, pp. 369–386.

Benbasat, I., and Zmud, R. W. 2003. "The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties," *MIS Quarterly*, pp. 183–194.

Benfeldt, O. 2018. "Theorizing the Problem of Data Governance: Findings from Danish Local Government," Unpublished master's thesis, Unpublished master's thesis, Aalborg, Denmark: Aalborg University.

Benfeldt, O., Persson, J. S., and Madsen, S. 2020. "Data Governance as a Collective Action Problem," *Information Systems Frontiers* (22:2), pp. 299–313.

Bennett, T., Holloway, K., and Farrington, D. P. 2009. "A Review of the Effectiveness of Neighbourhood Watch," *Security Journal* (22:2), pp. 143–155.

Berry, D. M. 2019. "Against Infrasomitization: Towards a Critical Theory of Algorithms," in *Data Politics: Worlds, Subjects, Rights*, D. Bigo, E. F. Isin, and E. Ruppert (eds.), London: Routledge, pp. 43–63.

Blædel, M. 2018. "Datalov Stresser Vaskefirma: Kunder Frygter Bøderegn," *Børsen*, p. 14.

Boonstra, A., Eseryel, U. Y., and van Offenbeek, M. A. 2017. "Stakeholders' Enactment of Competing Logics in IT Governance: Polarization, Compromise or Synthesis?," *European Journal of Information Systems*, Springer, pp. 1–20.

Breaux, T. D., and Alspaugh, T. A. 2011. "Governance and Accountability in the New Data Ecology," in *2011 Fourth International Workshop on Requirements Engineering and Law*, pp. 5–14.

Brous, P., Janssen, M., and Vilminko-Heikkinen, R. 2016. "Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles," in *International Conference on Electronic Government* (Vol. 9820), H. J. Scholl, O. Glassey, M. Janssen, B. Klievink, I. Lindgren, P. Parycek, E. Tambouris, M. A. Wimmer, T. Janowski, and D. Sá Soares (eds.), Cham: Springer International Publishing, pp. 115–125.

Brown, A. E., and Grant, G. G. 2005. "Framing the Frameworks: A Review of IT Governance Research," *Communications of the Association for Information Systems* (15), pp. 696–712.

Brown, C. V. 1999. "Horizontal Mechanisms under Differing IS Organization Contexts," *MIS Quarterly* (23:3), pp. 421–454.

Buffenoir, E., and Bourdon, I. 2013. "Reconciling Complex Organizations and Data Management: The Panopticon Paradigm," in *Proceedings - Pacific Asia Conference on Information Systems, PACIS 2013*.

Bygstad, B., Øvrelid, E., and Lie, T. 2018. *Establishing an Analytics Capability in a Hospital*, presented at the International Working Conference on Transfer and Diffusion of IT, Springer, pp. 3–14.

Cadwalladr, C. 2019. "The Great Hack: The Film That Goes behind the Scenes of the Facebook Data Scandal," *The Guardian*. (https://www.theguardian.com/uk-news/2019/jul/20/the-great-hack-cambridge-analytica-scandal-facebook-netflix).

Carlisle, K., and Gruby, R. L. 2017. "Polycentric Systems of Governance: A Theoretical Model for the Commons: Polycentric Systems of Governance in the Commons," *Policy Studies Journal*, pp. 1–26.

Cevea. 2017. "Ulighedens Danmarkskort 2017 | Indkomst." (https://cevea.dk/ulighedens-danmarkskort-2017-indkomst).

Chen, H., Chiang, R. H., and Storey, V. C. 2012. "Business Intelligence and Analytics: From Big Data to Big Impact.," *MIS Quarterly* (36:4), pp. 1165–1188.

Chen, H.-M., Schütz, R., Kazman, R., and Matthes, F. 2017. "How Lufthansa Capitalized on Big Data for Business Model Renovation.," *MIS Quarterly Executive* (16:1), pp. 19–34.

Child, J., and Rodrigues, S. B. 2003. "Corporate Governance and New Organizational Forms: Issues of Double and Multiple Agency," *Journal of Management and Governance* (7:4), Springer, pp. 337–360.

Coffey, A., and Atkinson, P. 1996. *Making Sense of Qualitative Data: Complementary Research Strategies.*, Sage Publications, Inc.

Constantinides, P., and Barrett, M. 2015. "Information Infrastructure Development and Governance as Collective Action," *Information Systems Research* (26:1), pp. 40–56.

Constantiou, I. D., and Kallinikos, J. 2015. "New Games, New Rules: Big Data and the Changing Context of Strategy," *Journal of Information Technology* (30:1), pp. 44–57.

Crawford, K., Miltner, K., and Gray, M. L. 2014. "Critiquing Big Data: Politics, Ethics, Epistemology," *International Journal of Communication* (8), pp. 1663–1672.

Cunliffe, A. L. 2002. "Reflexive Dialogical Practice in Management Learning," *Management Learning* (33:1), Sage Publications Sage CA: Thousand Oaks, CA, pp. 35–61.

Cunliffe, A. L. 2003. "Reflexive Inquiry in Organizational Research: Questions and Possibilities," *Human Relations* (56:8), Sage Publications, pp. 983–1003.

Cunliffe, A. L. 2011. "Crafting Qualitative Research: Morgan and Smircich 30 Years On," *Organizational Research Methods* (14:4), Sage Publications Sage CA: Los Angeles, CA, pp. 647–673.

DalleMule, L., and Davenport, T. H. 2017. "What's Your Data Strategy?," *Harvard Business Review*, pp. 2–13.

Daries, J. P., Reich, J., Waldo, J., Young, E. M., Whittinghill, J., Ho, A. D., Seaton, D. T., and Chuang, I. 2014. "Privacy, Anonymity, and Big Data in the Social Sciences," *Communications of the ACM* (57:9), pp. 56–63.

Data Protection Agency. 2018. "Årsberetning 2018."

Data Protection Agency. 2019. "Databeskyttelsesforordningen - Det Første År i Tal," *Datatilsynet*. (https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2019/maj/databeskyttelsesforordningen-det-foerste-aar-i-tal/).

Davenport, T. H. 2014. "How Strategists Use 'Big Data' to Support Internal Business Decisions, Discovery and Production," *Strategy & Leadership* (42:4), pp. 45–50.

Davenport, T. H., Barth, P., and Bean, R. 2012. "How 'Big Data' Is Different," *MIT Sloan Management Review* (54:1), pp. 43–50.

Davenport, T. H., and Bean, R. 2020. "Are You Asking Too Much of Your Chief Data Officer?," *Harvard Business Review*.

Davenport, T. H., and Patil, D. J. 2012. "Data Scientist: The Sexiest Job of the 21st Century," *Harvard Business Review*, pp. 70–82.

Dawes, S. S. 2010. "Stewardship and Usefulness: Policy Principles for Information-Based Transparency," *Government Information Quarterly* (27:4), pp. 377–383.

Dencik, L., Hintz, A., and Cable, J. 2016. "Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism," *Big Data & Society* (3:2), pp. 1–12.

Dencik, L., Hintz, A., Redden, J., and Treré, E. 2019. "Exploring Data Justice: Conceptions, Applications and Directions," *Information, Communication & Society* (22:7), pp. 873–881.

Digitaliseringsstyrelsen. 2017. "The Digitally Coherent Public Sector: White Paper on a Common Public-Sector Digital Architecture."

Digitaliseringsstyrelsen. 2018. "Fællesoffentlig Digital Arkitektur," *It-Arkitektur*. (https://digst.dk/data/it-arkitektur/, accessed July 30, 2018).

Dourish, P. 2017. *The Stuff of Bits: An Essay on the Materialities of Information*.

Economist. 2017. "The World's Most Valuable Resource," *The Economist*.

Elkjaer, B., and Simpson, B. 2015. "Pragmatism: A Lived and Living Philosophy. What Can It Offer to Contemporary Organization Theory?," in *Philosophy and Organization Theory* (Vol. 32), H. Tsoukas and R. Chia (eds.), Emerald Group Publishing Limited, pp. 55–84.

European Commission. 2018. *2018 Reform of EU Data Protection Rules*. (https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en).

European Union. 2016. "General Data Protection Regulation," *Official Journal of the European Union* (L119), pp. 1–88.

Farshid, S., Reitz, A., and Roßbach, P. 2019. "Design of a Forgetting Blockchain: A Possible Way to Accomplish GDPR Compatibility," in *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Fitzgerald, M. 2014. "How to Hire Data-Driven Leaders," *MIT Sloan Management Review*, p. 9.

Flyvbjerg, B. 2006. "Five Misunderstandings About Case-Study Research," *Qualitative Inquiry* (12:2), SAGE Publications Inc, pp. 219–245.

Fontana, A., and Frey, J. 1994. "Interviewing: The Art of Science," in *Handbook of Qualitative Research*, N. K. Denzin and Y. S. Lincoln (eds.), Thousand Oaks: Sage Publications.

Foster, K., Smith, G., Ariyachandra, T., and Frolick, M. N. 2015. "Business Intelligence Competency Center: Improving Data and Decisions," *Information Systems Management* (32:3), pp. 229–233.

Gabrys, J. 2019. "Data Citizens: How to Reinvent Rights," in *Data Politics: Worlds, Subjects, Rights*, D. Bigo, E. F. Isin, and E. Ruppert (eds.), Routledge.

Galliers, R. D., and Newell, S. 2001. "Back to the Future: From Knowledge Management to Data Management," *Back to the Future*, p. 7.

George, J. J., Yan, J., and Leidner, D. E. 2019. "Data Philanthropy: Corporate Responsibility with Strategic Value?," *Information Systems Management*, Taylor & Francis, pp. 1–12.

Getz, C. 1977. "Coalescence: The Inevitable Fate of Data Processing," *Mis Quarterly*, pp. 21–30.

Gioia, D. A., and Pitre, E. 1990. "Multiparadigm Perspectives on Theory Building," *Academy of Management Review* (15:4), pp. 584–602.

Girard, M., and Stark, D. 2002. "Distributing Intelligence and Organizing Diversity in New-Media Projects," *Environment and Planning A: Economy and Space* (34:11), pp. 1927–1949.

Goes, P. 2014. "Editor's Comments: Big Data and IS Research," *MIS Quarterly* (38:3), pp. iii–viii.

Goldkuhl, G. 2008. *Practical Inquiry as Action Research and Beyond.*

Goldkuhl, G. 2012. "Pragmatism vs Interpretivism in Qualitative Information Systems Research," *European Journal of Information Systems* (21:2), pp. 135–146.

Goodhue, D. L., Quillard, J. A., and Rockart, J. F. 1988. "Managing the Data Resource: A Contingency Perspective," *MIS Quarterly*, pp. 373–392.

Grover, V., and Lyytinen, K. 2015. "New State of Play in Information Systems Research: The Push to the Edges.," *Mis Quarterly* (39:2), pp. 271–296.

Gust, G., Neumann, D., Christoph, M., Brandt, T., and Philipp, P. 2017. "How a Traditional Company Seeded New Analytics Capabilities," *MIS Quarterly Executive* (16:3), pp. 215–230.

Guston, D. H. 2014. "Understanding 'Anticipatory Governance,'" *Social Studies of Science* (44:2), pp. 218–242.

Harari, Y. N. 2018. *21 Lessons for the 21st Century*, (First edition.), New York: Spiegel & Grau.

Hardin, G. 1968. "The Tragedy of the Commons," *Science* (162:3859), pp. 1243–1248.

Harris, J. G., Craig, E., and Egan, H. 2010. "How Successful Organizations Strategically Manage Their Analytic Talent," *Strategy & Leadership* (38:3), pp. 15–22.

Harris, J. G., and Mehrotra, V. 2014. "Getting Value from Your Data Scientists," *MIT Sloan Management Review*.

Hassan, N. R., and Lowry, P. B. 2015. *Seeking Middle-Range Theories in Information Systems Research*, presented at the International Conference on Information Systems (ICIS 2015), Fort Worth, TX, December, pp. 13–18.

Hess, C., and Ostrom, E. (eds.). 2007. *Understanding Knowledge as a Commons: From Theory to Practice*, Cambridge, Mass: MIT Press.

Hevner, A. R., March, S. T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly*, pp. 75–105.

Hintz, A., and Brown, I. 2017. "Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden," *International Journal of Communication* (11), pp. 782–801.

Hintz, A., Dencik, L., and Wahl-Jorgensen, K. 2018a. *Digital Citizenship in a Datafied Society*, John Wiley & Sons.

Hintz, A., Dencik, L., and Wahl-Jorgensen, K. (eds.). 2018b. "Challenging Datafication," in *Digital Citizenship in a Datafied Society*, Cambridge: Polity Press.

Holahan, R., and Lubell, M. 2016. "Collective Action Theory," in *Handbook on Theories of Governance*, J. Torfing and C. K. Ansell (eds.), Cheltenham, UK ; Northampton, MA: Edward Elgar Publishing, pp. 21–31.

Hook, D. W., Porter, S. J., and Herzog, C. 2018. "Dimensions: Building Context for Search and Evaluation," *Frontiers in Research Metrics and Analytics* (3), p. 23.

Huber, G. P. 1981. "The Nature of Organizational Decision Making and the Design of Decision Support Systems," *MIS Quarterly*, JSTOR, pp. 1–10.

Hvas, S. 2018. "Lønfirma Vendte GDPR-Frustration Til Succes," *Børsen*, p. 14.

Iliadis, A., and Russo, F. 2016. "Critical Data Studies: An Introduction," *Big Data & Society* (3:2), p. 205395171667423.

IT in Practice. 2019. "Digital & Technology - IT in Practice 2019-2020," Ramboll Management Consulting A/S.

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., and Janowski, T. 2020. "Data Governance: Organizing Data for Trustworthy Artificial Intelligence," *Government Information Quarterly*, Elsevier, p. 101493.

Jarlner, M. 2018. "Tech: Tilsyns-Dværge Skal Tøjle Datalystne Kæmpevirksomheder," *Politiken*, p. 10.

Johns, G. 2006. "The Essential Impact of Context on Organizational Behavior," *Academy of Management Review* (31:2), Academy of Management Briarcliff Manor, NY 10510, pp. 386–408.

Kang, C., and Vogel, K. P. 2019. "Tech Giants Amass a Lobbying Army for an Epic Washington Battle," *The New York Times*.

Kappelman, L., Torres, R., McLean, E., Maurer, C., Johnson, V., and Kim, K. 2019. "The 2018 SIM IT Issues and Trends Study," *MIS Quarterly Executive* (18:1), p. 7.

Kellogg, K. C., Orlikowski, W. J., and Yates, J. 2006. "Life in the Trading Zone: Structuring Coordination Across Boundaries in Postbureaucratic Organizations," *Organization Science* (17:1), pp. 22–44.

Khatri, V., and Brown, C. V. 2010. "Designing Data Governance," *Communications of the ACM* (53:1), p. 148.

Kieser, A., and Leiner, L. 2009. "Why the Rigour-Relevance Gap in Management Research Is Unbridgeable," *Journal of Management Studies* (46:3), pp. 516–533.

Kiron, D. 2017. "Lessons from Becoming a Data-Driven Organization," *MIT Sloan Management Review* (58:2).

Kiron, D., Prentice, P. K., and Ferguson, R. B. 2014. "The Analytics Mandate," *MIT Sloan Management Review* (55:4), p. 1.

Kjær, J. S. 2018a. "Firmaer Har Brugt 8 Milliarder På at Rydde Op Og Få Fokus På Databeskyttelse," *Politiken*, p. 6.

Kjær, J. S. 2018b. "Håndhævelse Af Datasjusk Halter," *Politiken*, p. 1.

Kjær, J. S. 2018c. "Her Er Danmarks Datasherif - Men Har Hun Patroner i Sin Revolver?," *Politiken*, p. 4.

Klein, H. K., and Myers, M. D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), pp. 67–94.

Knox, H., and Nafus, D. 2018. "Introduction: Ethnography for a Data-Saturated World," in *Ethnography for a Data Saturated World*, p. 30.

KOMBIT. 2018. "Monopolbruddet," *KOMBIT*, , March. (https://kombit.dk/monopolbrud, accessed March 25, 2020).

KOMBIT. 2020. "Den fælleskommunale infrastruktur," *Videncenter KL*. (https://videncenter.kl.dk/viden-og-vaerktoejer/rammearkitektur-og-infrastruktur/infrastruktur/, accessed July 27, 2020).

Kowalczyk, M., and Buxmann, P. 2015. "An Ambidextrous Perspective on Business Intelligence and Analytics Support in Decision Processes: Insights from a Multiple Case Study," *Decision Support Systems* (80), pp. 1–13.

Kurtz, C., and Semmann, M. 2018. *Privacy by Design to Comply with GDPR: A Review on Third-Party Data Processors*.

Ladley, J. 2012. *Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program*, Waltham, MA: Morgan Kaufmann.

Langefors, B. 1977. "Information Systems Theory," *Information Systems* (2:4), pp. 207–219.

Lee, A. S. 2001. "MIS Quarterly's Editorial Policies and Practices," *MIS Quarterly* (25:1), pp. iii–vii.

Lee, S. U., Zhu, L., and Jeffery, R. 2018. "A Data Governance Framework for Platform Ecosystem Process Management," *Lecture Notes in Business Information Processing* (329), pp. 211–227.

Lee, Y., Madnick, S., Wang, R., Zhang, H., and Wang, F. 2014. "A Cubic Framework for the Chief Data Officer: Succeeding in a World of Big Data," *MIS Quarterly Executive* (13:1), p. 6.

Levitan, A. V., and Redman, T. C. 1998. "Data as a Resource: Properties, Implications, and Prescriptions," *MIT Sloan Management Review* (40:1), p. 89.

Li, H., Yu, L., and He, W. 2019. "The Impact of GDPR on Global Technology Development," *Journal of Global Information Technology Management* (22:1), pp. 1–6.

Liaw, S.-T., Pearce, C., Liyanage, H., Cheah-Liaw, G. S., and De Lusignan, S. 2014. "An Integrated Organisation-Wide Data Quality Management and Information Governance Framework: Theoretical Underpinnings," *Journal of Innovation in Health Informatics* (21:4), pp. 199–206.

Littauer, M. L. 2018. "I Dag Får Du Lidt Af Magten over Dine Data Tilbage - Men Hvad Betyder Det?," *Berlingske*, p. 12.

Local Government Denmark. 2015. "Local and Digital - A Coherent Denmark. Common Municipal Digitalization Strategy 2016-2020."

Loebbecke, C., and Picot, A. 2015. "Reflections on Societal and Business Model Transformation Arising from Digitization and Big Data Analytics: A Research Agenda," *The Journal of Strategic Information Systems* (24:3), pp. 149–157.

Lycett, M. 2013. "'Datafication': Making Sense of (Big) Data in a Complex World," *European Journal of Information Systems* (22:4), pp. 381–386.

Maguire, J., and Winthereik, B. R. 2019. "Digitalizing the State Data Centres and the Power of Exchange," *Ethnos*, p. 29.

Marchand, D. A., and Peppard, J. 2013. "Why IT Fumbles Analytics," *Harvard Business Review* (91:1), pp. 104–112.

Markus, M. L. 2001. "Toward a Theory of Knowledge Reuse: Types of Knowledge Reuse Situations and Factors in Reuse Success," *Journal of Management Information Systems* (18:1), pp. 57–93.

Markus, M. L. 2015. "New Games, New Rules, New Scoreboards: The Potential Consequences of Big Data," *Journal of Information Technology* (30:1), pp. 58–59.

Marshall, A., Mueck, S., and Shockley, R. 2015. "How Leading Organizations Use Big Data and Analytics to Innovate," *Strategy & Leadership* (43:5), pp. 32–39.

Martin, K. E. 2015. "Ethical Issues in the Big Data Industry," *MIS Quarterly Executive* (14:2), pp. 67–85.

Mason, J. 2002a. "Organizing and Indexing Qualitative Data," in *Qualitative Researching* (2nd ed.), London ; Thousand Oaks, Calif: Sage Publications, pp. 147–165.

Mason, J. 2002b. *Qualitative Researching*, Sage.

Mathiassen, L. 2002. "Collaborative Practice Research," *Scandinavian Journal of Information Systems*, p. 33.

Mathiassen, L. 2017. "Designing Engaged Scholarship: From Real-World Problems to Research Publications," *Engaged Management ReView* (1:1).

Mathiassen, L., Chiasson, M., and Germonprez, M. 2012. "Style Composition in Action Research Publication," *MIS Quarterly*, JSTOR, pp. 347–363.

McAfee, A., and Brynjolfsson, E. 2012. "Big Data: The Management Revolution," *Harvard Business Review*, pp. 1–9.

McGinnis, M. D., and Ostrom, E. 2012. "Reflections on Vincent Ostrom, Public Administration, and Polycentricity," *Public Administration Review* (72:1), pp. 15–25.

McKinney, and Yoos. 2010. "Information About Information: A Taxonomy of Views," *MIS Quarterly* (34:2), p. 329.

Mikalef, P. 2017. "Big Data Analytics Capability: Antecedents and Business Value," *PACIS 2017 Proceedings*, p. 14.

Mikalef, P., Boura, M., Lekakos, G., and Krogstie, J. 2018. "Complementarities between Information Governance and Big Data Analytics Capabilities on Innovation," *Proceedings of the 26th European Conference on Information Systems*.

Mikalef, P., Boura, M., Lekakos, G., and Krogstie, J. 2020. "The Role of Information Governance in Big Data Analytics Driven Innovation," *Information & Management*, Elsevier, p. 103361.

Mikalef, P., and Krogstie, J. 2018. "Big Data Governance and Dynamic Capabilities: The Moderating Effect of Environmental Uncertainty.," in *Proceedings of the 22nd Pacific Asia Conference on Information Systems*, p. 206.

Mikalef, P., and Krogstie, J. 2020. "Examining the Interplay between Big Data Analytics and Contextual Factors in Driving Process Innovation Capabilities," *European Journal of Information Systems*, Taylor & Francis, pp. 1–28.

Mikalef, P., Pappas, I. O., Krogstie, J., and Pavlou, P. A. 2020. "Big Data and Business Analytics: A Research Agenda for Realizing Business Value," *Information & Management* (57:1), North-Holland, p. 103237.

Mindel, V., Mathiassen, L., and Rai, A. 2018. "The Sustainability of Polycentric Information Commons," *MIS Quarterly* (42:2), pp. 607–631.

Mingers, J. 1995. "Information and Meaning: Foundations for an Intersubjective Account," *Information Systems Journal* (5:4), pp. 285–306.

Mingers, J. 2001. "Combining IS Research Methods: Towards a Pluralist Methodology," *Information Systems Research* (12:3), pp. 240–259.

Mintzberg, H. 2005. "Developing Theory and the Development of Theory," in *Great Minds in Management: The Process of Theory Development*, K. G. Smith and M. A. Hitt (eds.), Oxford University Press, pp. 355–372.

Monteiro, E., and Parmiggiani, E. 2019. "Synthetic Knowing: The Politics of the Internet of Things," *MIS Quarterly* (43:1), pp. 167–184.

Morabito, V. 2015. "Big Data and Analytics," *Strategic and Organisational Impacts*.

Munkholm, M. 2018. "Ny Datalov Koster Virksomheder Milliarder," *Børsen*, p. 16.

Myers, M. D., and Newman, M. 2007. "The Qualitative Interview in IS Research: Examining the Craft," *Information and Organization* (17:1), pp. 2–26.

Myers, M. D., and Walsham, G. 1998. "Exemplifying Interpretive Research in Information Systems: An Overview," *Journal of Information Technology* (13:4), pp. 233–234.

Najjar, M. S., and Kettinger, W. J. 2013. "Data Monetization: Lessons from a Retailer's Journey.," *MIS Quarterly Executive* (12:4).

Neff, G., and Stark, D. 2004. "Permanently Beta," in *Society Online: The Internet in Context*, P. N. Howard and S. Jones (eds.), Sage, pp. 173–188.

Newell, S., and Marabelli, M. 2015. "Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification,'" *The Journal of Strategic Information Systems* (24:1), pp. 3–14.

Newell, S., Tansley, C., and Huang, J. 2004. "Social Capital and Knowledge Integration in an ERP Project Team: The Importance of Bridging AND Bonding," *British Journal of Management*, p. 15.

Nielsen, J. A., Mathiassen, L., and Newell, S. 2014. "Theorization and Translation in Information Technology Institutionalization: Evidence from Danish Home Care," *MIS Quarterly* (38:1), pp. 165–186.

Nielsen, O. B. 2017. "A Comprehensive Review of Data Governance Literature," *Selected Papers of the IRIS 40*, p. 15.

Nielsen, O. B., Persson, J. S., and Madsen, S. 2018. "Why Governing Data Is Difficult: Findings from Danish Local Government," in *Smart Working, Living and Organising*, A. Elbanna, Y. K. Dwivedi, D. Bunker, and D. Wastell (eds.), New York, NY: Springer Berlin Heidelberg, pp. 15–29.

Nielsen, P. A., and Persson, J. S. 2016. "Engaged Problem Formulation in IS Research," *Communications of the Association for Information Systems* (38), pp. 720–737.

Nokkala, T., Salmela, H., and Toivonen, J. 2019. "Data Governance in Digital Platforms," in *25th Americas Conference on Information Systems, AMCIS 2019*.

O'Reilly, K., and Paper, D. 2012. "Want Value from Big Data? Close the Gap between the C-Suite and the Server Room," *Journal of Information Technology Case and Application Research* (14:4), pp. 3–10.

Orlikowski, W. J. 1992. "The Duality of Technology: Rethinking the Concept of Technology in Organizations," *Organization Science* (3:3,), pp. 398–427.

Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the 'IT' in IT Research—A Call to Theorizing the IT Artifact," *Information Systems Research* (12:2), pp. 121–134.

OS2 - Offentligt digitaliseringsfællesskab. 2014. "Om OS2-fælleskabet." (https://os2.eu/side/om-os2, accessed July 27, 2020).

Ostrom, E. 1972. "Metropolitan Reform: Propositions Derived from Two Traditions," *Social Science Quarterly*, pp. 474–493.

Ostrom, E. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action*, The Political Economy of Institutions and Decisions, Cambridge ; New York: Cambridge University Press.

Ostrom, E. 2005. *Understanding Institutional Diversity*, Princeton University Press.

Ostrom, V. 1972. *Polycentricity*, presented at the 1972 Annual Meeting of the American Political Science Association, Washington, DC.

Ostrom, V., Tiebout, C. M., and Warren, R. 1961. "The Organization of Government in Metropolitan Areas: A Theoretical Inquiry," *American Political Science Review* (55:4), pp. 831–842.

Otto, B. 2011a. "Data Governance," *Business & Information Systems Engineering* (3:4), pp. 241–244.

Otto, B. 2011b. "Organizing Data Governance: Findings from the Telecommunications Industry and Consequences for Large Service Providers," *Communications of the Association for Information Systems* (29:1), pp. 45–66.

Otto, B. 2011c. "A Morphology of the Organisation of Data Governance," *ECIS 2011 Proceedings* (272), p. 13.

Otto, B. 2013. "On the Evolution of Data Governance in Firms: The Case of Johnson & Johnson Consumer Products North America," in *Handbook of Data Quality*, Springer, pp. 93–118.

Otto, B. 2015. "Quality and Value of the Data Resource in Large Enterprises," *Information Systems Management* (32:3), pp. 234–251.

Parmiggiani, E., and Grisot, M. 2020. "Data Curation as Governance Practice," *Scandinavian Journal of Information Systems* (32:1), p. 1.

Patton, M. Q. 2002. "Qualitative Interviewing," in *Qualitative Research & Evaluation Methods* (Fourth edition.), Thousand Oaks, California: SAGE Publications, Inc, pp. 339–419.

Pereira, G. V., Macadar, M. A., Luciano, E. M., and Testa, M. G. 2017. "Delivering Public Value through Open Government Data Initiatives in a Smart City Context," *Information Systems Frontiers* (19:2), pp. 213–229. (https://doi.org/10.1007/s10796-016-9673-7).

Persson, J. S., Reinwald, A. K., Skorve, E., and Nielsen, P. A. 2017. "Value Positions in E-Government Strategies: Something Is (Not) Changing in the State of Denmark," *Proceedings of the 25th European Conference on Information Systems*, pp. 904–917.

Polanyi, M. 1951. *The Logic of Liberty: Reflections and Rejoinders*, Routledge.

Porter, M. E., and Heppelmann, J. E. 2014. "How Smart, Connected Products Are Transforming Competition," *Harvard Business Review* (92:11), pp. 64–88.

Porter, M. E., and Heppelmann, J. E. 2015. "How Smart, Connected Products Are Transforming Companies," *Harvard Business Review* (93:10), pp. 96–114.

Porter, M. E., and Heppelmann, J. E. 2017. "A Manager's Guide to Augmented Reality," *Harvard Business Review* (95:6), pp. 45–57.

Power, E. M., and Trope, R. L. 2006. "The 2006 Survey of Legal Developments in Data Management, Privacy, and Information Security: The Continuing Evolution of Data Governance," *Bus. Law.* (62), p. 251.

Ransbotham, S., and Kiron, D. 2017. "Analytics as a Source of Business Innovation," *MIT Sloan Management Review*, p. 19.

Ransbotham, S., Kiron, D., and Prentice, P. K. 2016. "Beyond the Hype:The Hard Work Behind Analytics Success," *MIT Sloan Management Review*, p. 19.

Reeves, M. 2016. "On Infrastructural Indeterminacy and Its Reverberations," in *Infrastructures and Social Complexity : A Companion*, P. Harvey (ed.), Routledge.

Reidenberg, J. R. 2014. "The Data Surveillance State in the United States and Europe," *Wake Forest L. Rev.* (49), p. 583.

Rose, J., Hansen, A.-M., Aalborg Universitet, and Disimit (projekt). 2012. *IT Management in Local Government: The DISIMIT Project*, Aalborg: Aalborg University.

Rosenberg, M., Confessore, N., and Cadwalladr, C. 2018. "How Trump Consultants Exploited the Facebook Data of Millions," *The New York Times*.

Rosenberg, M., and Frenkel, S. 2019. "Facebook's Role in Data Misuse Sets Off Storms on Two Continents," *The New York Times*.

Russell, K. D., O'Raghallaigh, P., O'Reilly, P., and Hayes, J. 2018. *Digital Privacy GDPR: A Proposed Digital Transformation Framework*, presented at the AMCIS 2018-24th Americas Conference on Information Systems, Association for Information Systems, pp. 1–10.

Sabel, C. F., and Zeitlin, J. 2012. "Experimentalist Governance," *The Oxford Handbook of Governance* (1), pp. 2–4.

Sadowski, J. 2019. "When Data Is Capital: Datafication, Accumulation, and Extraction," *Big Data & Society* (6:1), p. 205395171882054.

Sambamurthy, V., and Zmud, R. W. 2000. "Research Commentary: The Organizing Logic for an Enterprise's IT Activities in the Digital Era—A Prognosis of Practice and a Call for Research," *Information Systems Research* (11:2), pp. 105–114.

Scheuer-Hansen, S., and Guldagger, M. 2018. "Forbrugerrådet: Brug to Minutter Og Få Kontrol over Dine Data," *Politiken*, p. 7.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action Design Research," *MIS Quarterly*, JSTOR, pp. 37–56.

Sharma, R., Mithas, S., and Kankanhalli, A. 2014. "Transforming Decision-Making Processes: A Research Agenda for Understanding the Impact of Business

Analytics on Organisations," *European Journal of Information Systems* (23:4), pp. 433–441.

Silver, M. S. 1991. "Decisional Guidance for Computer-Based Decision Support," *MIS Quarterly*, JSTOR, pp. 105–122.

Simon, H. A. 1973. "The Structure of Ill Structured Problems," *Artificial Intelligence* (4:3–4), pp. 181–201.

Skorve, E., Vassilakopoulou, P., Aanestad, M., and Grünfeld, T. 2017. "A Lens for Evaluating Genetic Information Governance Models: Balancing Equity, Efficiency and Sustainability," *Studies in Health Technology and Informatics* (235), pp. 298–302.

Solove, D. J. 2007. "I've Got Nothing to Hide and Other Misunderstandings of Privacy," *San Diego L. Rev.* (44), p. 745.

Solove, D. J. 2012. "Introduction: Privacy Self-Management and the Consent Dilemma," *Harv. L. Rev.* (126), p. 1880.

Stake, R. E. 1995. *The Art of Case Study Research*, sage.

Stamper, R. K. 1991. "The Semiotic Framework for Information Systems Research," in *Information Systems Research: Contemporary Approaches & Emergent Traditions: Proceedings of the IFIP TC8/WG 8.2 Working Conference on the Information Systems Research Arena of the 90's Challenges, Perceptions, and Alternative Approaches: Copenhagen, Denmark, 14-16 December 1990*, H.-E. Nissen, H.-K. Klein, and R. A. Hirschheim (eds.), Amsterdam ; New York : New York, N.Y., U.S.A: North-Holland ; Distributors for the U.S. and Canada, Elsevier Science Pub. Co, pp. 515–527.

Suddaby, R. 2010. *Editor's Comments: Construct Clarity in Theories of Management and Organization*, Academy of Management Briarcliff Manor, NY.

Susha, I., and Gil-Garcia, J. R. 2019. *A Collaborative Governance Approach to Partnerships Addressing Public Problems with Private Data*, presented at the Proceedings of the 52nd Hawaii International Conference on System Sciences.

Taddeo, M. 2016. "Data Philanthropy and the Design of the Infraethics for Information Societies," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* (374:2083), The Royal Society, p. 20160113.

Tallon, P. P., Short, J. E., and Harkins, M. W. 2013. "The Evolution of Information Governance at Intel.," *MIS Quarterly Executive* (12:4).

Taylor, L. 2017. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally," *Big Data & Society* (4:2), p. 205395171773633.

The Ministry of Justice. 2019. "Regeringen Udpeger Medlemmer Til Dataetisk Råd," *The Ministry of Justice*, , April 3. (https://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2019/regeringen-udpeger-medlemmer-til-dataetisk-raad).

Thompson, N., Ravindran, R., and Nicosia, S. 2015. "Government Data Does Not Mean Data Governance: Lessons Learned from a Public Sector Application Audit," *Government Information Quarterly* (32:3), pp. 316–322.

Tiwana, A., Konsynski, B., and Bush, A. A. 2010. "Research Commentary—Platform Evolution: Coevolution of Platform Architecture, Governance, and Environmental Dynamics," *Information Systems Research* (21:4), INFORMS, pp. 675–687.

Torfing, J., and Ansell, C. K. (eds.). 2016. "Introduction: Theories of Governance," in *Handbook on Theories of Governance*, Cheltenham, UK ; Northampton, MA: Edward Elgar Publishing, pp. 2–17.

Van de Ven, A. H. 2007. *Engaged Scholarship: A Guide for Organizational and Social Research*, Oxford University Press on Demand.

Van Dijck, J. 2014. "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology," *Surveillance & Society* (12:2), pp. 197–208.

Van Maanen, J. 2011. *Tales of the Field: On Writing Ethnography*, University of Chicago Press.

Vassilakopoulou, P., Pesaljevic, A., and Aanestad, M. 2018. "Polycentric Governance of Interorganizational Systems: Managerial and Architectural Arrangements," *ECIS 2018 Proceedings*.

Vassilakopoulou, P., Skorve, E., and Aanestad, M. 2019. "Enabling Openness of Valuable Information Resources: Curbing Data Subtractability and Exclusion," *Information Systems Journal* (29:4), Wiley Online Library, pp. 768–786.

Vilminko-Heikkinen, R., Brous, P., and Pekkola, S. 2016a. "Paradoxes, Conflicts and Tensions in Establishing Master Data Management Function," in *24th European Conference on Information Systems, ECIS 2016*.

Vilminko-Heikkinen, R., Brous, P., and Pekkola, S. 2016b. "Paradoxes, Conflicts and Tensions in Establishing Master Data Management Function," *ECIS 2016 Proceedings*, p. 17.

Vilminko-Heikkinen, R., and Pekkola, S. 2012. "Organizational Issues in Establishing Master Data Management Function.," in *ICIQ 2012*, pp. 1–13.

Vilminko-Heikkinen, R., and Pekkola, S. 2013. *Establishing an Organization's Master Data Management Function: A Stepwise Approach*, presented at the 2013 46th Hawaii International Conference on System Sciences, IEEE, pp. 4719–4728.

Vilminko-Heikkinen, R., and Pekkola, S. 2017. "Master Data Management and Its Organizational Implementation: An Ethnographical Study within the Public Sector," *Journal of Enterprise Information Management* (30:3), pp. 454–475.

Vilminko-Heikkinen, R., and Pekkola, S. 2019. "Changes in Roles, Responsibilities and Ownership in Organizing Master Data Management," *International Journal of Information Management* (47), pp. 76–87.

Vydra, S., and Klievink, B. 2019. "Techno-Optimism and Policy-Pessimism in the Public Sector Big Data Debate," *Government Information Quarterly*,

Walsham, G. 1995. "Interpretive Case Studies in IS Research: Nature and Method," *European Journal of Information Systems* (4:2), Taylor & Francis, pp. 74–81.

Walsham, G. 2006. "Doing Interpretive Research," *European Journal of Information Systems* (15:3), pp. 320–330.

Wang, R. Y., and Strong, D. M. 1996. "Beyond Accuracy: What Data Quality Means to Data Consumers," *Journal of Management Information Systems* (12:4), pp. 5-.

Wang, Y., Kung, L., Ting, C., and Byrd, T. A. 2015. "Beyond a Technical Perspective: Understanding Big Data Capabilities in Health Care," in *2015 48th Hawaii International Conference on System Sciences*, HI, USA: IEEE, January, pp. 3044–3053.

Weber, K., Otto, B., and Österle, H. 2009. "One Size Does Not Fit All - A Contingency Approach to Data Governance," *Journal of Data and Information Quality* (1:1), pp. 1–27.

Weick, K. E. 1989. "Theory Construction as Disciplined Imagination," *Academy of Management Review* (14:4), Academy of Management Briarcliff Manor, NY 10510, pp. 516–531.

Weick, K. E., Sutcliffe, K. M., and Obstfeld, D. 2005. "Organizing and the Process of Sensemaking," *Organization Science* (16:4,).

Weill, P. 2004. "IT Governance: How Top Performers Manage IT Decision Rights for Superior Results," *CISR Working Paper*.

Weill, P., and Ross, J. W. 2004. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business Press.

Wende, K. 2007. "A Model for Data Governance – Organising Accountabilities for Data Quality Management," *ACIS 2007 Proceedings*, p. 10.

Williams, C. K., and Karahanna, E. 2013. "Causal Explanation in the Coordinating Process: A Critical Realist Case Study of Federated IT Governance Structures," *Mis Quarterly*, pp. 933–964.

Williams, R. M. 1977. *Mutual Accommodation: Ethnic Conflict and Cooperation*, U of Minnesota Press.

Winter, J. S., and Davidson, E. 2017. "Investigating Values in Personal Health Data Governance Models," in *AMCIS 2017 Proceedings* (Vol. 23), p. 10.

Winter, J. S., and Davidson, E. 2018. "The Healthcare AI Juggernaut: Is PHI Data Governance Possible?," in *Living with Monsters? Social Implications of Algorithmic Phenomena, Hybrid Agency and the Performativity of Technology*, San Francisco State University.

Winter, J. S., and Davidson, E. 2019a. "Governance of Artificial Intelligence and Personal Health Information," *Digital Policy, Regulation and Governance* (21:3), pp. 280–290.

Winter, J. S., and Davidson, E. 2019b. "Big Data Governance of Personal Health Information and Challenges to Contextual Integrity," *Information Society* (35:1), pp. 36–51.

Winter, J. S., Davidson, E., Boyce, C., and Fan, V. 2019. "Emergence, Convergence, and Differentiation of Organizational Forms of Health Data Governance," in *Academy of Management Proceedings* (Vol. 2019), Academy of Management Briarcliff Manor, NY 10510, p. 16403.

Wixom, B. H., and Ross, J. W. 2017. "How to Monetize Your Data," *MIT Sloan Management Review* (58:3).

Woerner, S. L., and Wixom, B. H. 2015. "Big Data: Extending the Business Strategy Toolbox," *Journal of Information Technology* (30:1), pp. 60–62.

Yin, R. K. 2009. *Case Study Research: Design and Methods*, (4th ed.), Applied Social Research Methods, Los Angeles, Calif: Sage Publications.

Zigon, J. 2018. "Worldbuilding and Attunement," in *Disappointment: Toward a Critical Hermeneutics of Worldbuilding*, Fordham University Press, p. 208.

Zigon, J. 2019. "Can Machines Be Ethical? On the Necessity of Relational Ethics and Empathic Attunement for Data-Centric Technologies," *Social Research: An International Quarterly* (86:4), Johns Hopkins University Press, pp. 1001–1022.

Zuboff, S. 2015. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* (30:1), pp. 75–89.

Zuboff, S. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, (First edition.), New York: PublicAffairs.

ISSN (online): 2246-1256
ISBN (online): 978-87-7210-700-4 AALBORG UNIVERSITY PRESS