Organizations, state and power struggles in the age of digitalization and datafication

Obaid Amjad

http://hdl.handle.net/10803/689315

Data de defensa: 28-08-2023

UNIVERSITAT
RAMON LLULL

DOCTORAL THESIS

Title	Organizations, state and power struggles in the age of digitalization and datafication
Presented by	Obaid Amjad
Centre	Esade Business School
Department	Society, Politics and Sustainability
Directed by	Dr. David Murillo Bonvehí

Abstract

Digitalization and its related datafication processes have become an important line of inquiry in organizational research. This is owed to the fact digital technologies are becoming ubiquitous in the social sphere, and have a profound impact on shaping organizations, fields, and society alike. Recent literature is also problematizing the dark side of digitalization, which contributes to the growing power of corporations while subjecting citizens to disempowering positions. In acknowledging its growing influence across society, this thesis seeks to uncover the role of societal actors in both organizing and resisting the power of digitalization by exploring the following: how are relations of power and resistance organized between business, state, and citizens in relation to digitalization? After briefly making the case for such investigation in the introductory chapter, the second chapter undertakes a qualitative content analysis to uncover how resistance is organized against the datafication practices of corporations, as well as the efficacy of such challenges. The third chapter explores the role of the state in protecting citizens' online privacy through regulatory measures. The fourth chapter adopts a historical case study analysis to present a different side of the state, one which acts in tandem with economic actors and tech elites to promote digitalization in society. Taken together, this thesis reveals insights regarding how organized resistance and state action can both challenge and sustain the power of private corporations' datafication practices. Furthermore, the socially constructed nature of organizing digitalization is highlighted as an active site of persuasion and contestations between the involved actors.

To my family and friends

For my family and friends

Acknowledgements

My decision to pursue a PhD was rooted in my strong desire for intellectual stimulation and my passion for becoming a great teacher to inspire the forthcoming generation, who create a better world through their skillsets and compassion. As I approach the culmination of this journey, I myself have learnt so much and being profoundly inspired by the people involved in this great, at times a daunting, adventure. Indeed, life is not so much about the accomplishments but rather the people with whom they are shared to make them meaningful.

Firstly, I would like to extend my gratitude to my supervisor, Dr. David Murillo. David, your academic expertise and creativity are indeed well-renowned however, working with you exposed me to the caring and compassionate person that you are. The greatest thing that someone can offer another is their time and through my PhD journey, whenever I needed to speak to get some clarity or share some doubts, you always made sure that you were available to assist me. Your valuable and constructive feedback, encouragement during difficult times, humility, and kindness have been instrumental in allowing me to culminate this thesis. Due to your tutelage, I have indeed learnt to be humble while confident in my work, creative yet methodical and, above all, fair yet compassionate. Thank you David for being there every step of the way and truly being such an inspiring teacher. A great motivation for my future academic journey will be to make you proud. I would also like to thank the incredible faculty at the esade's Department of Society, Politics, Sustainability for making me feel at home, being genuinely invested in my academic success and, through their personal example, inspiring us to have highest levels of integrity. To Dr. Ignasi Marti, Dr. Daniel Arenas, Dr. Pep Maria, Dr. Arroyo: thank you for your time, support and care, through which I have come to understand the intricacies of academic life as well as the effort it requires to establish a great career. My academic journey could not have begun without the inspiring role that one of my professors during my Bachelor's degree played in my life. Professor Mohammad Keyhani has been a tremendous guide for me to not only navigate my way into academia but also as an inspiration for the kind of teacher I would like to become. Through his example, I have learned many valuable lessons that continue to shape me, both as an academic and as a person.

Secondly, the academic and convivial environment provided to PhD candidates at esade not only was a crucial support system, but also allowed me to feel at home. I would like to extend my gratitude to the head and administrators of the MRes and PhD programs – Dr. Sierra, Dr. Collet, Mrs. Gallego, and Mrs. Espin – for being invested in our success, and providing us with the facilities and resources to undertake our research.

During my academic journey, I had the fortune to work with two extremely special individuals – Dr. Rita Mota and Dr. Rebecca Ruehle – with whom I collaborated to create a Junior Scholars Network for the Society of Business Ethics, which serves as an informal platform to help junior-level scholars for academic and non-academic support. To both of you, your kindness and care is incredibly infectious, and I absolutely cherish working with you to create something that gives back to the academic community.

The PhD journey can indeed involve certain ups and downs, and no one understands them better than those who are also involved in a similar journey. I was blessed to have phenomenal colleagues as fellow PhD students, who have become dear friends and with whom I share a lasting bond. Rocio, Ali, Lucrezia, Vinicio, Lucie, Asma, Menna, Sahar, Amer, Zak, Atieh, Julia, Ipek, Shahzeb, Natalia, Marco, Matteo, Andreas, Edmund, Maosen, Yuqi, Yanbai, and all others: what a wonderful experience you made this PhD to be with your warmth and love, thank you!

There has not been a greater blessing in my life than my family and friends, a distinction with indeed very blurry boundaries. Khurram, Osama, Hasan: when have you ever not been there? Furre, Jon, Tim, Carmen, Waleed, Kamran, Saad, Hares, Adil, Carmen, Ana, Tim Best, Ali, Monsieur Chartillange: thank you!

To my immediate family, nothing that I have accomplished or will hopefully accomplish in the future would have been possible without your love and support. Farhan, Sara, Musab, Zaina, and Hassan, what an incredible blessing you all are. Amna, your warmth, kindness, and positivity have always pushed me through the difficult times. Omair, no person on this planet has believed in me as much as you have. Whether it was sports, school or changing careers, somehow you always believed that I could do it, even when I had doubted so. Ammi and Abbu, words fall short in thanking you for the sacrifices you have made in your lives for our sake. Your lives and example are the roadmap for the person that I wish I can become. Everything that I have, that I am, or ever will be, it is because of you and it will be for you. I love you!

Thank you all. Through your unique personalities and support, you were all great teachers who made possible this journey and inspired me.

Table of Content

List of Figures

List of Tables

Chapter 1. General Introduction

In recent years, scholarship in organizational studies is starting to pay due attention to digitalization and its impacts on organizing and society alike. While digitalization has become a widely used term, I draw on Leonardi and Treem's work which defines it as "*the ways in which social life is organized through and around digital technologies*" (2020, p. 1602). Digitalization, considered as a transformative process at organizational and societal levels (Bodrožić & Adler, 2022; Majchrzak et al., 2016; Trittin-Ulbrich et al., 2021), is made possible by the prevalence of ubiquitous digital technologies – electronic devices, systems, and resources – which are capable of creating, storing, and processing data (Martin, 2016a). Consequently, the processes of datafication, referring to "*the practice of taking an activity, behavior, or process and turning it into meaningful data*" (Leonardi & Treem, 2020, p. 1605), become intertwined with the concepts of digitalization and digital transformation.

With the proliferation of the internet, digital devices, and rise of online platforms, more and more activities of the personal, social, organizational, and political life are occurring in such settings and becoming subject to datafication processes (Couldry & Mejias, 2019; West, 2019; Zuboff, 2019). Digitalization has also become an imperative for organizations to leverage novel affordances such as improving their ability to enhance their internal processes, efficiently develop new products and services, and engage with their customer base (Hanelt et al., 2021; Kuusisto, 2017; McAfee & Brynjolfsson, 2012). Its dominant role in organizing can be captured by the fact that digitalization is no longer seen as a mere tool for organizations and institutions to employ, but that it is also shaping their very constitution (Alaimo, 2022; Faraj & Pachidi, 2021).

Nonetheless, the growing digitalization efforts of organizations and platforms have brought along with them various controversies and negative implications for citizens and societies, particularly pertaining to their datafication processes (Flyverbom et al, 2019; Zuboff, 2019; West, 2019). This thesis, in acknowledging this dark side of digitalization (Trittin-Ulbrich et al., 2021), seeks to focus on the organization of power related to and resistance against digitalization. In doing so, the power struggles between critical societal actors – such as corporations, the state, tech elites, and citizens – are highlighted in both constructing the power of digitalization as well as resisting its datafication practices. Given the ubiquity of digital technologies across all forms of life, uncovering these relations can indeed greatly contribute towards fostering responsible and ethical digital futures.

As corporations, which are now driven by an imperative of maximizing data extraction efforts, are a preeminent actor in the proliferation of digitalization (West, 2019; Zuboff, 2019), it is here that I believe it is important to discuss the rise of the regimes of datafication, before uncovering the novel opportunities that digitalization presents for organizing.

1.1. Surveillance capitalism – The regimes of datafication

Shoshana Zuboff, in her book *Surveillance Capitalism*, traces the rise of the data economy to the workings of Google in the aftermath of the dot-com bubble crash. In the early 1990s, the advent of the internet raised much intrigue and optimism regarding the potentialities of the internet. Such optimism was reflected in the rise of the dot-com bubble, wherein venture capitalists infused significant capital into start-up internet companies, especially relating to e-commerce and communications (Zott et al., 2011; Zuboff, 2019). However, in 2000, when many of these companies failed to become profitable, the dot-com bubble crashed. Google, facing pressure from their investors to increase profits, realized the value of the data that the search engine was collecting from its users' online activities. Such data, hitherto, was not considered an essential component of the business, which is reflected in the fact that the storage sites of such data were internally referred to as 'data exhausts' (Zuboff, 2019).

The company came upon a realization that such data offered potentialities for enhanced predictions about their users' behaviour, which could be utilized towards a targeted advertising revenue stream (Sadowski, 2019; West, 2019). This incentivized the search engine towards enhancing their data collection; in 2004, when Google became a publicly listed company in its first Initial Public Offering, it had become clear that Google was not a search engine but an advertising company (Zuboff, 2019). Hence, data collection as a primary activity of value creation started to gain traction. Seduced by its affordances, organizations became embroiled in valorizing the potential of data, with discourses such as 'data is the new oil' (Sadowski, 2019; The Economist, 2017) becoming commonplace in corporate strategies and business media discourse.

Given its potential to drive value creation, organizations and digital platforms are increasingly driven by an extraction imperative, wherein the goal is to enhance the conversion of citizens' personal and social engagements into meaningful data (Collier, 2020; West, 2019; Zuboff, 2019). Ultimately, in line with ubiquitous digitalization, all facets of human life are rendered, in the form of data, towards capitalist appropriation (Couldry & Mejias, 2019; Couldry & Yu, 2018; Thatcher et al., 2016). It is certainly noteworthy that even prior to the advent of digital technologies, capitalists had relied upon the use of data to enhance labour efficiency, depicted in the Taylorism methods of measuring workers' productivity and in the platformization of Toyota's automobile capitalism (Littler, 1978; Steinberg, 2022).

Where digitalization enhances this tendency is to supplement not only the magnitude of data collection through the ubiquity of digital technologies, but also through its simultaneity as datafication occurs in real-time (Sadowski, 2019; Trittin-Ulbrich et al., 2021). The data extraction imperative serves as the mechanism through which this new strand of capitalism seeks to expand its reach beyond the workspaces and convert all factors of human life into a site of capitalist production (Kassner et al., 2017). In the following section, I briefly delineate how the affordances of digitalization has made it a critical component for organizations to survive and secure competitive advantages.

1.2. Digitalization: An organizational necessity

As previously stated, corporations' valorization of data indeed has substantially increased their efforts to engage in its collection and processing (McAfee & Brynjolfsson, 2012). It has been posited that we are now living in the age of Big Data, which is defined as "*high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making*" (Ahmadi et al., 2016, p. 286). Digital technologies and the related datafication processes are becoming infused in organizational activities to enable novel forms of agility and learning (Kuusisto, 2017; Vial, 2019). I again highlight the affordances of digital technologies for organizing: they enable automated and real-time decision making, lead to enhancement of internal processes and customers' experiences, provide visibility over supply chains, serve as a tool for brand engagement, and open the doors for novel forms of innovation (Parida et al., 2019; von Krogh, 2018).

Furthermore, in addition to these opportunities for existing organizational structures, digitalization has also given rise to new business models, especially instantiated in the rise of digital platforms, which have challenged and shaped the composition of various organizational fields (Alaimo, 2022; Beverungen et al., 2019; Trittin-Ulbrich et al., 2021; Vial, 2019). Scholarly literature has enlightened us on the rise of file-sharing services such as Napster which challenged the dominance of record labels and ushered in an era of the platformization of music, recently illustrated by the growth of Apple Music and Spotify. Similarly, the accessibility of media content such as movies, television series, and news through digital channels reshaped the business models of longstanding service providers (Cho et al., 2016; Park, 2017).

As a result, the transformative power of digitalization for organizations, in either rendering dominant players obsolete or forcing their hands to effectively adapt their business models, highlights its primacy in an array of business settings (Andriole, 2017; Benner & Waldfogel, 2023; Correani et al., 2020; Hanelt et al., 2021). As indicated by Beverungen and colleagues (2019), digitalization has become embedded with the functioning of organizations so much so that they have assumed a taken-for-granted status.

1.3. Digitalization: A source of empowerment for citizens

While this thesis critically studies the shaping of power relations in the context of the dark side of digitalization and its associated datafication processes, it is important to highlight that such developments have also brought about positive implications for citizens (Etter et al., 2019; Whelan, 2013). The narratives of convenience and consumer power indeed have materialized in the digital realm as the ease of accessing information, entertainment content, online shopping and other services facilitate citizens' lives. Digital platforms – such as Amazon, YouTube, Facebook, Google, Twitter, Instagram, WhatsApp, TikTok, and Baidu among others – have become a part of the fabric of our daily functioning. For example, previously analog activities such as purchasing a book, applying for a job opportunity, paying bills, finding a romantic partner, and consuming news are taking place in online settings (Culnan & Bies, 2003; Labrecque et al., 2013; Muldoon, 2022; Trittin-Ulbrich et al., 2021).

Such convenience and improved users' experience have become important for citizens, which has heightened the need to digitalize from the demand side for corporations (Hanelt et al., 2021; Trittin-Ulbrich et al., 2021). We also witnessed the crucial role that digital technologies played during the Covid-19 pandemic by enabling citizens to continue working, as well as access healthcare and other services from the comfort of their homes (Alghamdi & Alghamdi, 2022).

Additionally, digitalization has activated 'new arenas of citizenship' which enable individuals and civil society actors such as social movements and activists to denounce power players – both the state and corporations – and propagate alternative futures (Birks, 2014; Castells, 2017). Given that digital platforms are driven by strong network effects, they can encourage the non-hierarchical exercise of voice against existing regimes of power to become arenas of public dissent (Castelló et al., 2013, 2016; Whelan, 2013). For example, we have witnessed digitally enabled movements such as MeToo and the Arab Spring revolution coalescing physically distant actors into unified, transcendent fronts against oppressive actors to bring about accountability and social change (Etter & Albu, 2021; Jamil, 2022; Rabindranath & Kapil, 2014). State power has also been challenged, such as through the WikiLeaks and the Snowden revelations, which exposed the power and invasiveness of the internet-industrial complex (Karatzogianni & Robinson, 2014). Furthermore, citizen activism has taken place on digital platforms against powerful corporations, including the very platforms that enabled such activism (Castelló et al., 2016; Trittin-Ulbrich et al., 2021).

Consequently, it can be posited that digital technologies have enabled new organizing possibilities, including for alternative organizing to the dominant capitalist regimes (Massa, 2017; Wilhoit & Kisselburgh, 2015). They allow individuals and civil society actors to redress the power imbalances in society and bring forth new concerns into the public arenas.

1.4. The dark side of digitalization: An avenue for inquiry

While acknowledging the positive potentialities of digitalization, I seek to draw due attention to how such technologies have also tilted the relations of power in society towards corporations, placing citizens in disadvantageous positions, often unbeknownst to them (Han, 2017). As highlighted in the case of Google's utilization of their users' data, digital technologies have been employed by corporations largely towards their profit maximizing objectives (Trittin-Ulbrich et al., 2021; West, 2019; Zuboff, 2019). Given the luring opportunities they offer to develop competitive advantages and open new streams of revenue from the capture of users' data (Martin, 2016a; West, 2019), platform power is truly captured in the rapid progression of technology companies becoming the biggest corporations in the world (Sadowski, 2019). However, such growth – often predicated on invasive datafication practices – has subjected users becoming data producing entities, as well as becoming the victims of the harmful uses of such data (Martin, 2016a; Wielki, 2015).

I reiterate that the imperative of maximum data extraction for corporations is accomplished by the surveillance of users' online, and in some instance offline, activities which are then converted into data for generating valuable insights (Elmholdt et al., 2021; Sadowski, 2019). Consequently, digital platforms are driven by their desire to maximize users' online engagements, which is facilitated by the ubiquity of digital technologies in our social world (Thatcher et al., 2016; Trittin-Ulbrich et al., 2021). Largely, such data extraction is conducted without the users' adequate awareness and consent of the extent of their surveillance (Martin, 2013, 2018; Martin, 2015), which highlights the lack of transparency involved in such processes (Albu & Flyverbom, 2019; Flyverbom, 2019; Flyverbom et al., 2019). Corporations, in accumulating data for capitalistic valorization (Sadowski, 2019), profit from privatizing the generated data objects in their possession, which represent intimate details of users' lives (Couldry & Mejias, 2019; Martin, 2016a; Miller & Weckert, 2000; Rainie et al., 2013; Thatcher et al., 2016). While users contribute with 'free' labor in the form of being subjected to datafication, it is corporations that are in a position to instrumentalize their efforts to generate significant financial returns for themselves.

Furthermore, the economic logics attached to digital technologies and the data extraction imperative also bring about negative implications regarding how the collected data is utilized (Couldry & Mejias, 2019; Thatcher et al., 2016; Trittin-Ulbrich et al., 2021). Prior research has highlighted that datafication is not only utilized to generate insights about users but also to nudge and manipulate their behaviours (Chen & Barnes, 2007; Christl & Spiekermann, 2016; Jesse & Jannach, 2021; Youn, 2009). In the economic realm, Google and Amazon are seen to direct digital traffic towards their own websites and products over those of competitors (Christl & Spiekermann, 2016). The ability of powerful actors to manipulate behaviours through data has also been witnessed in the social and political realm (Etter & Albu, 2021; Tufekci, 2008), most notably in the Cambridge Analytica controversy where Facebook data was utilized to manipulate users' voting preferences in the Brexit referendum and the 2016 US elections (Cadwalladr & Graham-Harrison, 2018). Such examples indicate that digitalization can pose a severe challenge to users' agency in their personal, economic and political lives (Greenwood & Cox, 2022).

Driven by their financial interests, these companies do not just generate significant financial returns but also exercise extraordinary social, political and economic power to reorient society and social institutions (Flyverbom et al., 2019; Whelan, 2019). As a result, the role of the state merits due attention. In the following section, I describe how state institutions seek to address the issues arising from digital corporations' emergent power.

1.5. Digitalization and the state

Given the growing power of digital platforms and corporations vis-à-vis their users, questions regarding how these actors and such technologies should be governed have come to the fore, especially in relation to the role of governments (Bodrožić & Adler, 2022; Flyverbom et al., 2019; Trittin-Ulbrich et al., 2021). Certainly, the governance of digitalization is characterized by an ambiguous approach from the state. The ubiquitous rise of digital technologies, in tandem with the spread of neoliberalism, was initially met with a largely non-interfering role of governments, especially in Western societies (Flyverbom et al., 2019; Micheli et al., 2020; Van Dijck, 2020; West, 2019). Scholarship has related the state's non-interference position to their dependency on the very data produced through the surveillance of private companies (Clarke, 2003; Trittin-Ulbrich et al., 2021).

Governments across the world have utilized such data for a variety of purposes, such as social planning, disaster management, and national security concerns among others. For example, in the United States, following the 9/11 attacks, mass-scale surveillance of citizens was enabled through the Patriot Act; these objectives relied on shadowing the online-offline activities of the groups in questions (Karatzogianni & Robinson, 2014). As much of the internet remains within the control of private companies, governments have fostered a close relationship with the tech sector. This is referred to as the internet-industrial complex, which marks a marriage between Big Brother and Big Data to create "*a powerful and very difficult-to-reverse set of social forces around the expansion of mass surveillance and commodification of personal information*" (Flyverbom et al., 2019, p. 11).

However, the rising privacy violations and the growing discontent of civil society against these practices have reengaged the state (Cammaerts & Mansell, 2020; Chenou & Radu, 2019; Finck, 2018; Knudsen & Moon, 2017). Private corporations sought to evade regulatory oversight by valorizing the supremacy of self-regulation, highlighting that their expertise power makes them more suitable to address the controversies arising from the technical complexities of digitalization and datafication than the state (Berg, 2019; Bowie & Jamal, 2006; Parsons, 2019). Furthermore, in promoting hybrid governance forms, these private actors dominate the formulation of state regulations, which reasserts their power vis-à-vis the state and leads to the obfuscation of important ethical issues related to their functioning (Chenou & Radu, 2019; Finck, 2018). For example, in relation to the issue of the prevalence of fake news on social media platforms, Trittin-Ulbrich and colleagues highlight that "*these organizations are often keen to avoid governments regulations, and instead prefer to work with 'fact checkers' to ward off the risk of governments becoming more involved in censoring their activities*" (Trittin-Ulbrich et al., 2021, p. 15). Nonetheless, the datafication practices of private actors has become a critical issue in the public domain which has invited sterner reengagement of state action, such as the European Union's (EU) General Data Protection Regulation (GDPR).

Indeed, it becomes imperative to acknowledge the important role of the state in curbing the power of these corporations in the age of digitalization.

Until this point, I have delineated how digitalization, despite many positive affordances, also carries a dark side wherein private corporations, uninhibited by state power, are able to exert much influence in society at the expense of citizens. Hence, it becomes critical to address questions relating to how power relations in society are organized and shaped in the age of digitalization. To redress the growing power imbalances tilted in favour of private corporations, challenges from alternative organizations, civil society, and the state merit further attention to critically examine the societal impact of digital technologies (Flyverbom et al., 2019; Micheli et al., 2020).

1.6. The need to understand power struggles in the age of digitalization

Given the aforementioned challenges related to digitalization and its associated datafication processes, there is a great need to understand the organization and shaping of power relations amongst important societal actors, which both resist and naturalize the said developments. This thesis aims to respond to this essential topic. By power relations, I refer to both the concepts of power – not in its episodic exercise but rather its systemic nature (Fleming & Spicer, 2014) – and resistance (Mumby, 2005; Mumby et al., 2017). It is, hence, crucial to indicate the interrelations between these terms and highlight their relevance for the digital context.

The construct of power has been utilized in organizational settings for decades however, Fleming and Spicer (2014) delineate the array of meanings associated with it, along with their operationalization. Power can be exercised within, against or through organizations, referring to how organizations, their members, as well as external actors or stimuli shape and themselves are shaped by each other (Bloomfield & Hayes, 2009; Fleming & Spicer, 2014). Power can either be episodic, in that it can be directly exercised through identifiable acts to shape behaviours such as coercing or manipulating actors towards particular endeavours (Fleming & Spicer, 2014). However, I am interested in the systemic focus of power, which influences behaviours and activities through mobilizing institutional, discursive, and ideological resources to naturalize relations of power (Fleming & Spicer, 2014). As a result, the systemic form of power is certainly more invisible and difficult to challenge. This highlights the deep connection between power and ideology, which refers to "*a set of beliefs about how the social world operates, what outcomes are desirable and how they can be best achieved*" (Kwon &

Constantinides, 2018, p. 25; Seeck et al., 2020). In fact, it has been highlighted that ideology cannot be interchanged for institutional logics, as the latter does not account for the systemic nature of ideas and the associated power dimensions (Seeck et al., 2020).

The exercise of power, be it episodic or systemic, can invite resistance from an array of social actors. Resistance refers to "*an effort to engage in some form of praxis – individual or collective, routine or organized – in the context of established social patterns and structures (including mechanisms of control), such that these patterns are, at some level, dereified*" (Mumby, 2005, p. 23). It is crucial to discuss that power does not exclude resistance acts. In fact, Foucault highlights that "*where there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power*" (1978, p. 95). However, such a perspective has been critiqued due to the issue of embedded agency, whereby resistance to dominant structures is indeed shaped by power, rendering productive resistance as not viable (Fleming & Spicer, 2003, 2008; Gill, 2008). It is here that organization studies have fallen into the trap of the 'banality of resistance', whereby cynical and benign acts are valorized as resistance to reinforce the dominant systems in place (Contu, 2008; Fleming, 2016). Nonetheless, in acknowledging the dominance of existing regimes of power, scholarship has also shown that transformative resistance can indeed be fostered from within and outside of organizations to generate new futures and possibilities which tilt the balance of power (Baikovich et al., 2021; Courpasson, 2017; Ybema & Horvers, 2017).

While previous literature has shown that digitalization imbues itself in society through its affordances of solutionism and enabling efficiency (Hensmans, 2021; Muellerleile & Robertson, 2018), the power and resistance dynamics between critical societal actors in relation to it is a domain that requires further attention in organization studies (Flyverbom et al., 2019). Further investigations into the naturalization of and contestation to digitalization and datafication activities through the state-business-civil society nexus can provide crucial insights into how digitalization and its associated datafication can shape societies, as well as revealing possibilities towards alternative modes of organizing. Consequently, this thesis aims to address the following research question: *how are relations of power and resistance organized between business, state, and citizens in relation to digitalization*? In undertaking this challenge, we aim to shed light on the role of the state both as an enabler of digitalization and as the protector of citizens' privacy, as well as the organized resistance which is formulated to counter the data-driven business models. The following section describes the structure of this thesis.

1.7. Structure of the thesis

This thesis contains five chapters. The first and the fifth chapter respectively correspond to the introduction and conclusion, while the second, third and fourth chapter each examine the unique relationships between businesses, the state and the civil society actors in naturalizing and resisting digitalization and datafication processes. Chapter 2 undertakes a qualitative content analysis to investigate the offerings of self-proclaiming data activist entities that problematize and claim to resist the datafication practices of private corporations. After analyzing the offerings proposed by these entities, they are then categorized them into three resistance strategies through which the datafication practices of corporations are contested. The contradictory and productive faces of resistance (Mumby et al., 2017) are then delineated in scrutinizing the resistance strategies to show how resistance against datafication can often be dependent on the very datafication processes that are problematized, while offering potentialities towards both naturalizing and de-naturalizing the ideological work that enables unhindered datafication by private actors. In doing so, this chapter looks at how the powerful datafication regime is resisted by market and civil society actors, such as social movements and advocacy groups.

Building upon the insights from Chapter 2, the next two chapters highlight the double-edged role of the state (Trittin-Ulbrich et al., 2021) in both resisting datafication (Chapter 3) as well as hegemonizing digitalization in society (Chapter 4). The entities examined in the second chapter valorized the data rights provided by the EU's GDPR, which forms the setting for the conceptual piece in Chapter 3. In highlighting the privacy violations that are carried out by private corporations to accumulate vast amounts of users' data (Martin, 2012, 2013, 2015, 2016a, 2018), the third chapter of this thesis examines the efficacy of the GDPR to protect citizens' informational privacy, especially in relation to four critical controversies that render them powerless. Whereas privacy concerns have been highlighted from a variety of scholars, we employ a normative understanding of privacy as a social contract of informational exchange (Martin, 2016b), wherein users' expectations regarding data collection and its subsequent uses are honoured. In analyzing the GDPR through the social contracts lens of privacy, the dynamic nature of privacy is promoted in the digital arena to empower users while the burdensome self-management of privacy is posited as a critical issue in keeping citizens in the roles of dispossessed actors. This chapter, hence, highlights the interaction between political institutions' intervention to protect citizens against the datafication practices of private corporations.

The fourth chapter of this thesis highlights the other side of the state, which is seduced by the affordances of digitalization and is involved in socially constructing and promoting it within society (Beyes et al., 2022). In adopting a historical case study analysis, this chapter explores a national-level digitalization drive to highlight the dynamic and shifting governing role of the state, as well as its alliances with the technology experts and the private sector. Adopting a neo-Gramscian lens, the chapter exposes how the ideology of technosolutionism (Morozov, 2013) and the cult of technique – referring to the primacy of efficiency in modern capitalist states (Ellul, 1964) – entice the development of digital infrastructure and services, which is organized through the persuasion and coercion tactics by the state and private actors towards the populace. Resultantly, this chapter sheds greater light on the acknowledged, but less studied, alliance between state and digital experts, through which digitalization is naturalized at a social level to overcome contestations and resistance from civil society actors and citizens.

The following sections summarize the theoretical approaches, methods, and findings of the three core chapters of this thesis, while also illustrating the plan and schedule for their publication in academic journals. The fifth and final chapter discusses the theoretical and practical implications of this thesis, while also delineating the limitations and avenues for future research. The references for this and the concluding chapter of the thesis are presented at the end of the final chapter whereas the references for the core chapters – Chapter 2, 3, and 4 – are presented at the end of each chapter respectively.

1.7.1. Chapter 2

The second chapter employs the concept of resistance (Fleming, 2016; Mumby, 2005; Mumby et al., 2017) to understand how entities, which position themselves as data activists, seek to counter the datafication practices of private corporations. Whereas resistance to digital platforms has largely focused on how alternative platforms reproduce capitalism (Ossewaarde & Reijers, 2017) and enable the precarity of gig economy workers (Bucher et al., 2021; Peticca-Harris et al., 2020; Walker et al., 2021), the underlying datafication processes that enable platform power are largely overlooked. As resistance is contextual (Mumby et al., 2017), this chapter seeks to contribute to such literature by understanding the challenges, as well as assessing their complicity, to the accumulation by dispossession datafication processes (Couldry & Mejias, 2019; Thatcher et al., 2016) of digital platforms. Particularly, the following questions are addressed: *How is resistance organized against the dispossessive corporate accumulation in the form of datafication? How does the organized resistance challenge and/or* *reproduce the existing regimes of data colonialism?* Corresponding to the objective of this thesis, this study enables visibility into how the systemic power of digital platforms, captured through their datafication processes and its underlying ideological work, is resisted by those organizations and initiatives that aim to empower citizens.

After explicating the literature on resistance and the ideological work of the datafication regime through the literature on data colonialism (Couldry & Mejias, 2019; Thatcher et al., 2016), we undertake a qualitative content analysis methodology to inductively derive seven action items of these entities through which they seek to de-reify the data extraction practices of private corporations, which are then submerged into three overarching strategies of resistance: (i) resistance through breaking enclosures and challenging data monopolies, (ii) resistance through denaturalizing and politicizing datafication, and (iii) resistance through sheltering from data extraction. The employment of the qualitative content analysis methodology relates to the need to remain close to the collected data, while delineating a snapshot of the resistance strategies through rigorous categorical refinement (Flick & Schreier, 2014). Thereafter, we track the data flows associated with the three resistance strategies to enable a deeper understanding of the dependencies and challenges posited by the examined entities to reveal what we term as the Janus face of resistance, revealing the contradictory logics embedded in all acts of resistance.

This chapter, in its examination of the resistance against the ideological underpinning of datafication regimes of private corporations, responds to calls to examine the power relations associated with accumulation by dispossession processes in the digital realm (Van Lent et al., 2021) and offers an intervention against the systemic power of digital platforms. The findings reveal the confrontational and complicit nature of resistance in the novel digital context, revealing how state action – in particular the data rights granted through the GDPR – as well as narratives of citizens' empowerment lead to the fragmentation of resistance. Avenues for denaturalizing the imperceptible nature of datafication and sheltering citizens from such processes are posited as promising avenues to politicize datafication and lead towards alternative, promising futures to challenge platform power.

1.7.2. Chapter 3

Leveraging the findings from the second chapter wherein data rights are valorized as a critical component of breaking data monopolies, the third chapter of this thesis examines the role of political institutions in countering platform power. Scholarship has highlighted how the datafication processes associated with digitalization have posed severe challenges to users' privacy, which is considered a basic human right (Bowie & Jamal, 2006; Obar, 2020). In continuously being exposed to datafication, citizens find themselves in disempowered positions in relation to private corporations, which conduct surveillance of their digital activities for datafication, to be utilized for instrumental aims. However, studies investigating how citizens' privacy in the digital realm is protected through state and political institutions' regulatory actions remain scant. Hence, in line with the aim of this thesis, Chapter 3 investigates how the EU's GDPR – the manifestation of a political institution's action against the power of private corporations – safeguards its citizens' informational privacy. Specifically, the following research question is addressed: *What expectations can digital users hold of the GDPR in its role of empowering them through greater protection of their data?* To address this question, this essay explicates a normative understanding of privacy as a social contract (Martin, 2016b), wherein due attention is given to the context and expectations of informational exchange. This is especially enabled through the core procedural principles of (i) informed consent, (ii) voice and (iii) exit, that can enable fair data exchanges. Thereafter, we delineate four major privacy violations that result in the disempowerment of users vis-à-vis private corporations.

This chapter, then, analyzes how the GDPR enables the maintenance of citizens' informational privacy and protects them from the main privacy violations by strengthening the procedural principles of privacy. The assessment of the GDPR reveals the necessity for a dynamic view of privacy in the age of datafication, making them involved actors in relation to their data. As a result, the concept of privacy can be seen as an arena of politics, not only to challenge the datafication processes of platforms but also to curb their power post-datafication by enabling greater ownership of the created data. Nonetheless, implications regarding how state actions can overburden users through promoting self-management of data are also discussed (Obar, 2015).

1.7.3. Chapter 4

Whereas Chapter 2 and 3 discuss how the datafication practices of private corporations are challenged through alternative organizations and state action, they do not fully capture the role of the state in being a proponent of digitalization, especially due to the congruence of interests with the private sector (Flyverbom et al., 2019; Trittin-Ulbrich et al., 2021). While this marriage of interests is highlighted in the scholarly literature, the fourth chapter of this thesis aims to highlight the mindsets and ideologies associated with digitalization that shape the organization of a state-level digitalization drive. Digital technologies have been shown to embody capitalistic ideologies focused at a meso-level (Hensmans, 2021; Peticca-Harris et al., 2020; Walker et al., 2021) however, there have been growing calls for systemic level analyses to shed light on the role of public policy, the state, and other actors in organizing digitalization within society (Bodrožić & Adler, 2022). Certainly, investigating at a macro level can shed light on the overlooked role of the state – accounting for its interactions with businesses and civil society actors – to organize digitalization initiatives.

As a result, in Chapter 4, we adopt a neo-Gramscian approach – employing a qualitative, historical case study based on interviews and archival data – to investigate the organization of Estonia's digitalization drive. Upon its liberation from the Soviet Union, Estonia leveraged the affordances of digital technologies to modernize its infrastructure and has strongly promoted its national identity as being an advanced digital nation. Hence, this setting presents a fertile setting to assess the role of various actors in the organization of digitalization at a societal level. We utilize the concept of hegemony, which refers how social forces utilize coercion and consensus-building strategies to naturalize particular worldviews – digitalization in this instance – as advantageous (Gramsci, 1971; Levy & Egan, 2003; Morton, 2007). In particular, we address the following questions: *what role do state-business-civil society actors play in promoting digitalization within society? How does this nexus shape the desires of the masses and limit contestations in relation to digitalization?* The historical case study methodology enables us to highlight the dynamic and changing role of the state in promoting digitalization over a 16-year period, which involved surrendering control to the tech elite and strategies to both coerce and persuade the masses towards the value of digital technologies. Hence, this chapter enables critical insights into how digitalization is naturalized through the state-business nexus (Flyverbom, 2019) towards the masses.

1.8. Conference presentations and publishing strategy

Table 1.1 captures how Chapter 2, 3, and 4 of this thesis are currently in various stages of the publication process. Chapter 2 and 3 have been presented in various academic conferences, such as European Group of Organizational Studies, Society for the Advancement of Socio-Economics, and Academy of Management while an early version of Chapter 4 was presented at the International Association for Business and Society. The second chapter of the thesis has been submitted to *Organization*, while Chapter 3 is currently being reworked for a special issue in *Academy of Management Perspectives* for October 2023. Chapter 4 is currently being prepared for friendly reviews, with the aim of submitting it to *Organization Studies*. As the lead author for these projects, I have been responsible for the development of these chapters, relating to formulation of the research questions, conducting the literature review, data collection and analyses.

Table 1.1: Contributions to scientific knowledge

Title	Journal	Status	Conference Seminars and Presentations
Janus in the digital trenches: Resisting data extractivism through complicity and confrontation	Organization	Submitted	Society for the Advancement of Socio-Economics Annual Conference2019 38th EGOS Colloquium 2022
Setting the Expectations Right: Reassessing the Power of GDPR in Protecting Online Users' Privacy	Academy of Management Perspectives	To be submitted in October 2023	Society for Business Ethics Annual Conference 2020 Academy of Management Annual Meeting 2020 35th EGOS Colloquium 2019
Digital Hegemony: Uncovering the role of the state in Estonia's Digitalization	Organization Studies	To be submitted in September 2023	International Association for Business and Society Annual Conference 2021

Chapter 2. Janus in the digital trenches: Resisting data extractivism through complicity and confrontation

2.1. Abstract

Corporate accumulation by dispossession, studied prior in postcolonial contexts, is also embedded in the data extraction processes of digital platforms and corporations, typified by what is known as data colonialism. In this chapter, we seek to understand how resistance is organized against such dispossessing data extraction practices. Towards this end, we conduct a qualitative content analysis of the offerings of those self-proclaiming data activist organizations that claim to resist data extractivism. Our analysis reveals three broad resistance strategies employed by these entities: resistance through breaking enclosure and challenging data monopolies, resistance through denaturalizing and politicizing datafication, and resistance through sheltering from data extraction. We contribute to the literature on resistance by scrutinizing these strategies to reveal the 'Janus face of resistance' against data colonialism; in paying due attention to the ideological work of data colonialism, we highlight how resistance efforts can confront the dominant systems and yet be complicit in reproducing them.

2.2. Introduction

Janus, the Roman deity, symbolizes duality. Usually depicted as having two faces – one looking forward and the other looking backward, one optimistic and the other pessimistic – Janus represents contrasting aspects of a single entity, often at odds with one another

(Wikipedia, Collins Dictionary of American English)

Resistance against corporate accumulation has largely been examined in organization studies from a postcolonialism lens whereby the dispossession of indigenous communities, deprived of their natural and cultural resources, invites opposition from these subjugated actors (Banerjee et al., 2021; van Lent et al., 2021; Varman & Al-Amoudi, 2016). The inexorable rise of the internet, communication technologies, and digital platforms have given rise to new possibilities for corporate accumulation in the form of data extractivism (Couldry & Mejias, 2019; West, 2019; Zuboff, 2019). Corporations are now being driven by the imperative of continuous and maximum extraction of the data produced through enhanced surveillance of citizens' online engagements (Couldry & Mejias, 2019; Thatcher et al., 2016). Critical data scholarship has likened the practices of such data accumulation to a form of data colonialism (Couldry & Mejias, 2019; Thatcher et al., 2016) marked by the same processes of "accumulation by dispossession" that are studied in postcolonial literature (Banerjee, 2008;

Banerjee et al., 2021; Harvey, 2003), whereby citizens are now deprived of the data they produce by powerful corporate actors.

Following the call from Van Lent and colleagues (2021), this chapter seeks to understand how resistance is organized in the digital context against the data extractivist practices of corporations. Resistance literature has focused on a wide array of individual and collective praxis through which dominant neoliberal work regimes (Courpasson et al., 2012; Daskalaki & Kokkinidis, 2017; Fleming, 2016; Fleming & Spicer, 2003a, 2008; Taskin et al., 2022), ultraorthodox religious institutions (Baikovich et al., 2021), or oppressive regimes (Marsh & Śliwa, 2021; Martí & Fernández, 2013) can be challenged. The outcome of such resistance can paradoxically sustain the dominant systems being resisted (Contu, 2008; Fleming, 2016; Mumby et al., 2017) as well as transform them (Baikovich et al., 2021; Courpasson et al., 2012).

While resistance against digital platforms in organization studies has primarily focused on the efforts of precarious gig economy workers (Peticca-Harris et al., 2020; Pignot, 2021; Walker et al., 2021), critical organizational scholarship has largely overlooked the organization of resistance against data extractivism. Given the contextual nature of resistance (Mumby et al., 2017), we seek to fill this gap to enrich the organizational scholarship on resistance, especially in the context of corporate accumulation of data.

Various organizations have emerged that problematize these underlying datafication processes. As these organizations can enrich the critical scholarship on resistance by highlighting datafication processes as an important site of resistance, we consequently analyze their offerings and narratives with the following research question driving our efforts: *how is resistance organized against the dispossessive corporate accumulation in the form of datafication? How does the organized resistance challenge and/or reproduce the existing regimes of data colonialism?*

Towards this end, in this chapter, we examine the forms of resistance as exposed in the offerings of an array of data activist organizations to understand the actions and strategies through which they seek to challenge data extractivism. Our analysis reveals that these entities seek to confront the dispossessive corporate accumulation of data through three overarching strategies: (i) through breaking enclosures and challenging data monopolies, (ii) through denaturalizing and politicizing datafication, and (iii) through sheltering from data extraction.

Our study contributes to the resistance literature by highlighting the ‘Janus face of resistance’ which can be both complicit and confrontational, as various acts by the examined entities reproduce the ideological underpinning of data colonialism and develop an entrenched dependency on the very datafication structures they seek to resist. We also advance the literature on the fragmentation of resistance through individualization by highlighting that resistance is not just weakened through the hopelessness of individual actors but also through a form of smart power (Han, 2017) which valorizes them and seduces them through benefits. Additionally, we highlight that in the digital context, data mobility can simultaneously contribute towards resistance that is directed towards the individual as well as society, blurring the dichotomization of resistance acts as either individual or collective. Lastly, we enhance the literature on resistance against corporate accumulation by exploring these processes in relation to a resource (personal data) that is easily replicable and discuss the consequences of data replication for repossession.

The chapter proceeds as follows. First, we explore the literature to explicate data extractivism as a form of corporate accumulation through dispossession before unpacking the study of resistance in organization studies to make the case for how our context can enrich the extant scholarship. Next, we detail the criteria for collecting the sample for our study before describing our analysis strategy that enabled us to derive and scrutinize the resistance strategies offered. Thereafter, we present our findings, highlighting the various types of resistance presented by the examined initiatives. In the discussion section, we shed light on the Janus face of resistance to posit our contributions to scholarship.

2.3. Theoretical background

2.3.1. Data extraction as a contemporary form of dispossession

Corporate accumulation processes have largely been studied in postcolonial and critical organization studies to highlight the dispossession of indigenous communities’ natural and cultural resources by capitalist and colonialist organizations (Banerjee, 2008; Banerjee et al., 2021; van Lent et al., 2021; Varman & Al-Amoudi, 2016). Driven by their desire to commoditize and marketize these resources, historical and contemporary organizations have been incentivized to maximize their extractive tendencies through converting “public domains (e.g., natural resources) into private property” (van Lent et al., 2021, p. 4), leading to a system of ‘accumulation by dispossession’ (Harvey, 2003; Wurst, 2015).

In addition to natural resources (Banerjee et al., 2021; van Lent et al., 2021; Varman & Al-Amoudi, 2016), Van Lent and colleagues have called for greater investigation towards understanding dispossessive accumulation around "contemporary contexts includ[ing] the new forms of marketization around digital spaces (Couldry & Mejias, 2019) …which create organizational attempts at primitive accumulation that involve legitimation and resistance" (2021, p. 21). As corporate extractivist efforts induce resistance from the subjugated communities, in this chapter, we seek to understand how resistance is organized against the data extractivism practices of digital platforms, which exemplify the digital version of such processes of accumulation by dispossession.

We draw upon the work of Couldry and Mejias (2019), and Thatcher and colleagues (2016) on data colonialism to illustrate how these practices are naturalized and constitute accumulation by dispossession of citizens' data. Corporate accumulation in the digital arena unleashes its power to instrumentalize human experiences at the most granular and individuated level in the form of data (Couldry & Mejias, 2019; Thatcher et al., 2016; West, 2019). As the value derived from data increases with its quantity and variety, digital platforms operate on the imperative of maximum data extraction (Couldry & Mejias, 2019; West, 2019). The ubiquity of digital platforms and tools offering a wide array of services – such as social media, news outlets, dating platforms, fitness tracking – commoditize and privatize human life towards capitalist appropriation: "data colonialism paves the way for a new stage of capitalism…the capitalization of life without limits" (Couldry & Mejias, 2019, p. 336).

The accumulation by dispossession processes implicated in data appropriation rely on ideological work and discursive practices performed by corporations and institutional actors to naturalize the datafication of citizens' online activities. The extractivist rationality compares data to a resource like oil which simply 'exists' in these environments rather than being actively produced (Couldry & Mejias, 2019). Social rationalities are employed to further naturalize the datafication processes as a form of data 'sharing'. Potential resistance is also countered through a political rationality that presents society as the main beneficiary of such extractivist efforts by highlighting the benefits of online communities, personalized services, and consumer power (Couldry & Mejias, 2019; Thatcher et al., 2016; West, 2019).

If corporate accumulation of colonialist organizations is performed at the level of communities and employs hard power in the form of violence, coercion, and threats (Banerjee et al., 2021; van Lent et al., 2021; Varman & Al-Amoudi, 2016), in the digital realm, the data to be extracted has to be created individually by citizens by encouraging their engagement online. Hence, the dispossessed actors are not threatened through hard power but what Han (2017) refers to as 'smart power' where citizens are seduced through notions of freedom and pleasure, which are then exploited and appropriated in the form of data.

Accumulation by dispossession ensues as the data appropriated from citizens' online engagements is privatized in the possession of the platforms: "accumulation by dispossession fundamentally entails making private of something previously not" (Thatcher et al., 2016, p. 995). In addition to the aforementioned ideological practices, the privatization of citizens' data is enacted through incomprehensible end user license agreements and terms of service, which institutionalize the privatization of the produced data through claims of acquiring of citizens' consent (Couldry & Mejias, 2019; Thatcher et al., 2016; West, 2019).

Given its pervasiveness, the context of dispossessive data accumulation presents an intriguing opportunity to inquire about the new types of resistance that seek to confront such accumulation by dispossession. To aid us towards this goal, in the next section, we review the literature on resistance as presented in the field of organization studies.

2.3.2. Resistance in organization studies

Resistance has been defined as "*an effort to engage in some form of praxis – individual or collective, routine or organized – in the context of established social patterns and structures (including mechanisms of control), such that these patterns and structures are, at some level, dereified*" (Mumby, 2005, p. 23). Resistance is organized in response to the economic, social and ethical threats faced by actors, which mobilizes them to become political and act to counteract the oppressive regimes in place (Fleming, 2016). The dominant structures are challenged through a variety of resistance acts, which Mumby and colleagues (2017) dichotomize as either individual or collective, as well as either covert or overt.

Organizational scholarship has largely studied resistance within and around organizations, focusing on the efforts of employees to resist domination by the hegemonic neoliberal workplace (Courpasson et al., 2012; Fleming, 2016; Fleming & Spicer, 2003a). Resistance within these structures is often seen to romanticize a defeatist perspective (Fleming, 2016), whereby individuals employ hidden and secretive actions, and discourses to prevent a colonization of their selves, leading to a 'banality of resistance' (Fleming, 2016; Fleming & Spicer, 2003a, 2008). Such notions are also reproduced in the literature pertaining to digital platforms in the gig economy, where gig workers are rendered powerless against the 'invisible algorithmic management' and employ tactics such as venting, derision, and laughter to cope with their precariousness (Peticca-Harris et al., 2020; Pignot, 2021; Walker et al., 2021).

Resistance and power structures are closely interconnected in complex and often contradictory ways, whereby they are co-constitutive, as acts of resistance often reproduce and strengthen the hegemonic relations they seek to alter (Contu, 2008; Mumby et al., 2017). As Foucault highlights, "*where there is power, there is resistance, and yet, or rather consequently, this resistance is never in a position of exteriority in relation to power*" (1978, p. 95). Hence, embedded agency is often problematized as an obstacle to generate productive resistance (Fleming & Spicer, 2003a; Mumby et al., 2017).

However, in recognizing that resistance occurs within dominant structures, recent work has also exposed how organizational actors – both individually and collectively – position themselves within these regimes to acquire legitimacy and create change from within (Baikovich et al., 2021; Courpasson et al., 2012; Ybema & Horvers, 2017). Baikovich and colleagues (2021) highlight that compliance forms an integral aspect of altering the prevalent power structures, as resisting actors maintain their membership and legitimacy to enact change from within. Similarly, it is highlighted that translocal practices – involving the mobility of personnel and resources – are critical in cultivating resistance through solidarity initiatives to *reconfigure* previously enclosed and privatized spaces into collective, political arenas of citizenship (Daskalaki & Kokkinidis, 2017).

Consequently, resistance must also be understood in relation to the setting in which is occurs – minor acts of defiance in one context may not be seen as resistance in less, extreme contexts (Fleming, 2016; Marsh & Śliwa, 2021; Martí & Fernández, 2013; Mumby et al., 2017). In the context of corporations' and colonizers' accumulation of natural and cultural resources through dispossession, resisting actors deploy a variety of tactics such as guerilla warfare (van Lent et al., 2021) or discursive efforts to invoke their defenselessness (Varman & Al-Amoudi, 2016). However, in the digital context, given the ideological work and use of 'smart power' (Han, 2017), the perceptibility of the dispossessing accumulation of citizens' data remains low which can enervate resistance against such practices. Nonetheless, new organizations which posit themselves as data activists are emerging, seeking to present challenges to the data practices of corporations. Availing this opportunity, we seek to understand how resistance is organized against the dispossessive datafication practices of corporations and how it informs current discussions on contestation in the digital realm.

2.4. Methods

2.4.1. Sample

Following the logic that dispossessive data extractivism is premised upon instrumentalizing large amounts of data (Couldry & Mejias, 2019; West, 2019), we sought to compile a list of those digital platforms and initiatives which were specifically engaged in data activism related to the citizens' data itself being the 'object of struggle' (Beraldo & Milan, 2019) and/or situated themselves as challenging the data extractivist practices of corporations. Towards this goal, we created an initial exploratory list by overviewing the most recognizable joint research projects and activist movements based on media and scholarly attention – i.e., MyData Global, DataEthics, DECODE project, Ranking Digital Rights and the Electronic Frontier Foundation (Karppinen & Puukko, 2020; Lehtiniemi & Ruckenstein, 2019) – compiling the names and information of various data activist entities they highlighted.

We supplemented this initial exploratory list through conducting general web searches and reviewing specialized press to identify 137 initiatives; however, to respond specifically to our research question, our sample followed further criteria for selection. Those initiatives that were not explicitly and predominantly focusing on the digital citizens' data were removed from the list, such as AI-focused service provisioning, ID verification services, e-commerce and online payment services, and business-to-business solutions. Through these efforts, as well as excluding those entities about whom sufficient information was not easily available, we were able to finalize a sample of 32 digital entities – personal data management solutions, social movements and advocacy groups, education initiatives, data cooperatives and alternative service providers – which we utilize to understand how resistance is organized to challenge dispossessing data extractivism.

Our sample, predominantly comprised of European-based entities, contains both for-profit and non-profit organizations and was compiled in line with the insights from alternative organizing scholarship, which highlights that dominant regimes must be challenged through a wide array of practice, whose prefigurative potential must be adequately assessed (Wright, 2018; Zanoni, 2020). Some of the examined entities have since become de-active however, their strategies to resist the dispossessive data extraction remain operational by other entities in our sample. Table 2.1 contains the name and description of these entities.

2.4.2. Data analysis

Adopting a qualitative content analysis strategy (Van Den Brink et al., 2010), our analysis was text-based, comprising of the information exposed on the websites of the data activist entities selected. Web-based content analysis in the field of organization studies has proven useful to understand the offerings and strategies of organizations relating to CSR and sustainability reporting (Jose & Lee, 2007; Wu et al., 2010). Although the websites were examined closely, generally the sections of particular interest to us included: a) the Home page b) the 'About Us' page which captures the values; c) the mission statement of the selected initiatives; d) the webpages capturing details of the offered services and

Table 2.1: List of entities analyzed

Name	Description
Personal Data Marketplace/Store/Exchange	
CitizenMe	A personal information management (PIM) service which empowers digital citizens with their personal data
Cozy Cloud	A personal cloud server to store your data and install web apps in a user-controlled space
Data for Good Foundation	A data foundation and public health project enabling greater control for citizens
Datacoup	A platform for data exchange that puts citizen in control and their data's chief beneficiaries
Datangoo	A platform that offers quizzes to gather data as donations for NGOs and social causes
Digi.me	An API/app for private data sharing under enhanced control and privacy
Fair & Smart	A personal data management solution aiming to promoting transparent and balanced relationships
HIE OF ONE	An open-source project for personal data exchange in US healthcare sector
Meeco	A personal data ecosystem (Me-economy) to manage digital relationships and create mutual value
MesInfos	A project that aims to get citizens' data back and store it in CozyCloud
Mydex	A personal data ecosystem to management personal data and realize data's potential value
Pdata Token	A decentralized platform for democratic brokerage of personal data
VETRI	A blockchain-enabled personal data management and exchange platform
Social Movements and Advocacy	

ClaimyourData	An awareness group that engages multiple stakeholders to make data rights meaningful
Data Ethics EU	A ThinkDo Tank offering knowledge exchange for sustainable and ethical data future
MyData Global	A social movement connecting local hubs
PersonalData.IO	An advocacy group offering tools for personal data management
Personal Data Ecosystem Consortium	A non-for-profit trade association that promotes citizen-centered data logistics
Education/Training/Toolkits	
Inrupt	A project to decentralize the web and the commercial ecosystem behind Solid
Privowny	A personal data coach to create digital memory and manage personal information
Solid	A set of tools and conventions for building decentralized social applications
Tactical Technology Collective	A non-profit organization that offers toolkits for data detoxication, provides training and focuses on data ethics
Terms of Service; Didn't Read	A web platform that translates Terms & conditions in an understandable form
Trackography	An interactive map that shows users where their data is moving and through which company when they read news
Who Targets Me	A Github plugin to learn who targets digital users to influence their voting patterns
Alternative Service Providers	
diaspora*	A decentralized, alternative social network focusing on freedom and privacy
Snips AI	A platform for building your own AI-powered voice assistant with decentralized technology
StartMail	An e-mail service focusing on state-of-the-art privacy-enhancing technologies
Tresirut	A secure, personal cloud and storage service
Data Cooperatives	
MiData	A platform cooperative that enables citizens to actively manage their health data
Salus Coop	A citizen-governed health data cooperative
Savvy Coopearative	A health data cooperative that conducts interviews and quizzes with citizens, and enables them to sell this information

e) their aspirational principles, if present, as well as transcripts of the videos they contained. We focused on these sections as they hold the "inventory" of the key content and messages the data activists sought to deliver (Pauwels, 2012, p. 252).

We employed a two-step strategy for our analysis. In the first stage, we were interested in understanding the narratives, offerings, and strategies through which the examined entities claimed to resist data extractivism. Towards this end, we proceeded by inductively deriving categories from the data (Hsieh & Shannon, 2005; Strauss & Corbin, 1990). First, we imported the data on Atlas.ti software and familiarized ourselves with it, before open coding it to identify emerging themes while remaining close to the data (Strauss & Corbin, 1990). For example, 'facilitating exercise of data rights' was used to describe activities related to actions that helped citizens to exercise greater control over their data through data rights.

Then, the first order codes were compiled into second-order themes, which aimed to distinctly capture the actions taken by the examined entities. These codes were iteratively reviewed and analyzed by the two authors to overcome disagreements and achieve categorical distinction. Lastly, the action items were further refined and categorized into three overall strategies presented by the examined entities to challenge the data extractivism of platforms. Table 2.2 captures the results of this step, highlighting the various strategies to challenge data extractivism along with their associated action items, complemented with illustrative quotes.

In the second step, we posited these categories in relation to the dispossessing data production processes of corporations to highlight how they engage with and challenge them. This step involved engaging with the literature and data to chart the 'data flows' to identify patterns of dependency on and contestation against dispossessive accumulation of data (Lehtiniemi, 2017), which are captured in Figure 2.1. As a result, we were able to theorize distinct modes of resistance, through which the examined entities sought to challenge data extractivism, which we use to organize our findings and discussion.

2.5. Findings

In this section, following from our analysis, we highlight the three strategies and their related action items employed by the examined entities to organize resistance against the dispossessive corporate accumulation of data, along with their interconnections with the very dominant structures they claim to resist.

2.5.1. Strategy 1: Resistance through breaking enclosures and challenging data monopolies

Various entities that we have examined critique the corporate accumulation of citizens' data and present it as a critical democratic failure, whereby the corporations instrumentalize citizens' data while depriving them of what they produce.

> *"Already the five most valuable companies in the world - Alphabet (Google's parent company), Amazon, Apple, Facebook and Microsoft - deal, primarily, in data. They are valued based not on their assets but on the power that comes from their ability to gather and manipulate massive quantities of data"* (ClaimYourData)

Table 2.2: Resistance strategies emerging from coding process

Strategy	Corresponding Action	First Order Codes	Illustrative Quotes
Strategy 1: Resistance through breaking enclosures and challenging data monopolies	Enfranchising the individual through state mobilization	Presenting State as a weak actor Facilitating exercise of data rights Establishing standards with data holders for data portability and access rights Informing government committees on data ethics and rights	"*Our laws have not followed pace with the technological evolution, which means that legally you can today do a lot with data that is not in the best interest of the individual. This leads to an increasing data asymmetry and information power imbalance, which is a democratic problem in essence*" (Data Ethics EU) "*In many countries, individuals have enjoyed legal data protection for decades, yet their rights have remained mostly formal: little known, hard to enforce, and often obscured by corporate practices. We want true transparency and truly informed consent to become the new normal for when people and organisations interact. We intend access and redress, portability, and the right to be forgotten, to become "one-click rights": rights that are as simple and efficient to use as today's and tomorrow's best online services*" (MyData Global) "*The GDPR, which comes into force in the UK (and other Eu countries) on 25th May 2018, requires any organisation in the UK that holds our personal data – any data they hold that is linked in any way to us as individuals – to "return" this to us in a useable form (so-called "data portability"). This is an important new right."* (Claim Your Data) "*We provide expert advice on digital rights to regulators and policymakers at the local and regional levels of government. Our input has informed discussions at the European Parliament, Council of Europe, UK Parliament, US Senate, and more*" (Personal Data)
	Reclaiming data, reclaiming capital	Promote decentralized data architectures: personal data homes Import data produced on other platforms: Enable citizens to avoid vendor lock-in and prevent exploitation of data	"*Cozy is the first digital home on the market. It gives users an intelligent, decentralized and secure storage space that allows them to retrieve information via its connectors (photos, bank statements, operator invoices, e-merchants, etc.)*" (Cozy Cloud) "*INDIVIDUAL AS THE POINT OF INTEGRATION The value of personal data grows exponentially with their diversity; however, so does the threat to privacy. This contradiction can be solved if*

			individuals become the "hubs" where, or through which cross-referencing of personal data happens" (MyData Global) *"Because applications are decoupled from the data they produce, users will be able to avoid vendor lock-in, seamlessly switching between apps and personal data storage servers, without losing any data or social connections"* (Solid)
	Democratizing the surplus	Facilitating data exchanges Personalized insights and benefits for citizens Contribute data to market research and social projects Data monetization	"*Up until now the power to capture, analyse and profit from personal data has resided with business, government and social networks. What if you and I had the same power?*" (Meeco) "*All the current projects are carefully selected to develop and test the legal, ethical and technological framework that will provide a means of a fair and transparent data access that respects the autonomy and privacy of patients/citizens*." (MiData) "*We are currently helping individuals and service providers use personal data to better manage chronic health conditions, access debt advice, improve independent assisted living and assure identities*" (MyDex) "*Help those who sell ideas and products get it right more often or break some ground by taking part in medical research*" (CitizenMe) "*We wanted to give you the tools to help you sell your data, so your data profile also has a public link that you can share with potential purchasers.* " (DataCoup)
Strategy 2: Resistance through denaturalizing and politicizing datafication –	Educating to expose exploitation in data industry	Education about the data industry Explicating privacy policies	*"This workshop gives participants the chance to explore the reasons why online privacy is important to them. Through discussions and hands-on application, participants are introduced to the data collection industry and take concrete steps to live a more private life online."* (Data Detox Kit) "*We are a user rights initiative to rate and label website terms & privacy policies, from very good Class A to very bad Class E. Terms of service are often too long to read, but it's important to understand what's in them. Your rights online depend on them. We hope that our ratings can help you get informed about your rights*" (Terms of Service; Didn't Read)

Countering the Information Asymmetries	Exposing datafication through datafication	Recording the digital traces left on websites through browser plugins Explicate what information is collected and where it is held Engage other social actors to raise social awareness about and politicize datafication	“*You create an anonymous profile (age, gender, location, political leaning) and continue to use Facebook as normal. The software collects the Facebook adverts you see and adds them to the Who Targets Me database. Once you start to see political adverts, it provides you with a personalised breakdown of those posts, along with links to them, and information about why you were targeted with that advert.”* (Who Targets Me) “*The Data Manager automatically captures the trail of personal information left on websites. It offers users some visibility over their digital footprint. It allows them to remain aware of who they shared information with and what information each website has compiled about them*” (Privowny) *“The data collected through Trackography is open and can serve as a resource for researchers, lawyers, activists, advocates, campaigners and digital security trainers who are interested in raising critical questions about third party trackers or who want to show what happens to our data online”* (Trackography)
Strategy 3: Resistance through sheltering from data extraction	Avoidance of data capture in service delivery	Zero-knowledge privacy Offline data storage Direct transfer of produced data to decentralized data storage space	“*Zero-knowledge No one, not even Tresorit, can look into the content of your files* ” (Tresorit) “*Instead of everyone’s data being held on huge central servers owned by a large organization, diaspora* exists on independently run servers (“pods”) all over the world …In diaspora* you own your data. You don’t sign over rights to a corporation or other interest who could use it*” (diaspora*)
	Buttressing the defenses - Promoting tools for data circumvention	Guidelines to avoid datafication Blocking third party trackers	*“The smart thieves are out there, and the same are insurance companies, so do not write on your 'doorstep' that you're not home”* (Data Ethics EU).

Figure 2.1: Charting the data flows involved in the resistance strategies

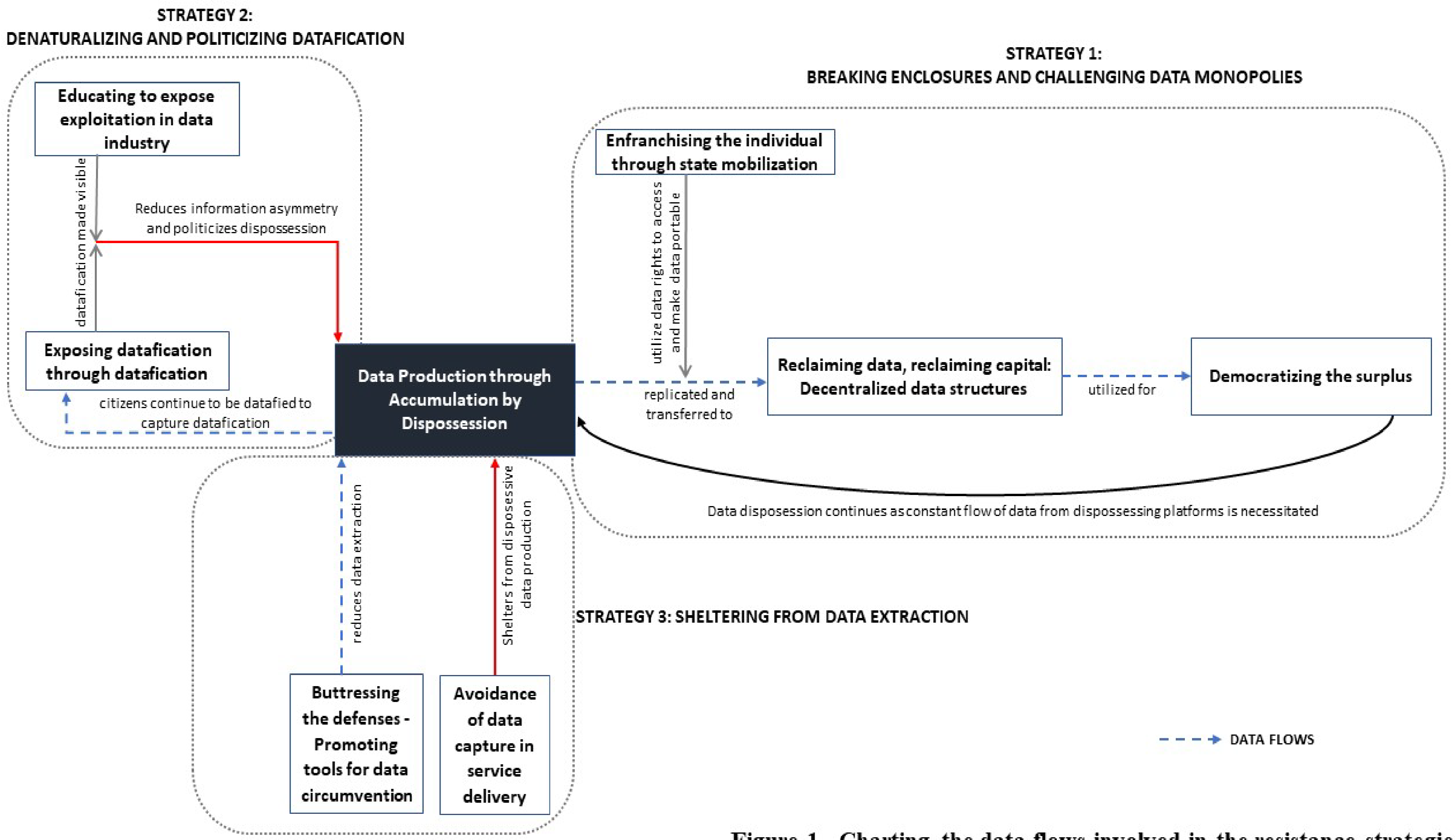

STRATEGY 2:
DENATURALIZING AND POLITICIZING DATAFICATION
Educating to expose exploitation in data industry
datafication made visible
Reduces information asymmetry and politicizes dispossession
Exposing datafication through datafication
citizens continue to be datafied to capture datafication
Data Production through Accumulation by Dispossession
STRATEGY 1:
BREAKING ENCLOSURES AND CHALLENGING DATA MONOPOLIES
Enfranchising the individual through state mobilization
utilize data rights to access and make data portable
replicated and transferred to
Reclaiming data, reclaiming capital: Decentralized data structures
utilized for
Democratizing the surplus
Data disposession continues as constant flow of data from dispossessing platforms is necessitated
reduces data extraction
Shelters from dispossessive data production
STRATEGY 3: SHELTERING FROM DATA EXTRACTION
Buttressing the defenses - Promoting tools for data circumvention
Avoidance of data capture in service delivery
DATA FLOWS

Figure 1 - Charting the data flows involved in the resistance strategies

One main avenue to challenge data monopolies implies mobilizing the state to enfranchise the citizen through promoting post-datafication rights to contest enclosure and enable greater access over the data they produce.

2.5.1.1. Action 1: Enfranchising the individual through state mobilization

Some of the entities present the state as an ineffective actor to counter the datafication practices of corporations:

> "*Our laws have not followed pace with the technological evolution which means that legally you can today do a lot with data that is not in the best interest of the individual. This leads to an increasing data asymmetry and information power imbalance, which is a democratic problem in essence*" (Data Ethics EU).

Consequently, these entities – largely social movements and advocacy groups – seek to confront the dispossessive datafication processes in the digital realm by activating the state. They do so through valorizing existing legislations as well as directly shaping state action. These actions do not directly confront the dispossessive data production processes but rather, the focus is largely on promoting the provision of personal data rights post-datafication, which are seen as enabling citizens to gain access to 'copies' of their data they produce and exercise more control over them.

Predominantly based in Europe, some of the analyzed entities celebrate the data rights provided in the European Union's General Data Protection Regulation (GDPR) and assert their commitment to facilitate the exercise of these rights. As corporations obscure these rights through incommodious processes filled with technical jargon, some of these entities (MyData Global and Fair&Smart) envision and provide solutions to make data rights – such as rights to access, portability and in some instances, erasure – more easily accessible as *"one-click rights"*. In catering to citizen's time and cognitive limitations, PersonalData also serves as liaisons for citizens to access, move or erase their data from digital platforms.

Specifically, these organizations highlight data mobility through the rights of access and portability, which return personal data to citizens, as a critical challenge to the dispossessing datafication processes of corporations as it *"gives [the citizen] more control and visibility over who and how our data is being used"* (Claim Your Data). Envisioning that "*the temptation will be for large data holders to undertake minimal compliance*", Claim Your Data seeks to engage data holding entities to "*establish standards for data sharing in digital form*" – such as the format of the returned data – so that citizens can easily avail their rights. Such actions indicate that these data activists aim to valorize the existing state legislation by enhancing the efficacy and enforceability of post-datafication rights.

Along with strengthening existing state action, some of the examined entities seek to directly engage state actors to promote greater data ethics. Entities such as Data Ethics EU and Personal Data operate knowledge-oriented foundations and actively participate in state-level initiatives, bringing their expertise to various levels of the government to inform and shape data ethics standards and data legislations. Their discursive approach fills the knowledge gap of regulators and upholds the salience of data rights to ensure that the ungoverned digital landscape sees greater state action. Data Ethics EU has promoted values of citizens' self-determination, transparency, and accountability of data processes to various governments' committees, such as European Data Protection Supervisor's Digital Ethics Board, United Kingdom's Council of Data Ethics, the Danish Government's Data Ethics Expert Committee, and the European Commission. Similarly, Personal Data's activities include serving as advisors to inform the less-savvy regulators on discussions related to data rights: their "*input has informed discussions at the European Parliament, Council of Europe, UK Parliament, US Senate, and more*".

Our analysis reveals that the examined entities are largely seen to focus on the retrieval of access to the data that citizens produce whereas the very countering dispossessive datafication processes, such as through promoting data minimization, remain largely absent from their narratives, with the exception of MyData Global.

2.5.1.2. Action 2: Reclaiming data, reclaiming capital

Availing the opportunities provided by state legislations that enable citizens to access their own data, many of the examined entities greatly promote and facilitate the re-appropriation of personal data.

Critiquing digital platforms for accumulating and restricting access to citizens' data in centralized databases, several data activists underscore the importance of citizens reclaiming their personal data and promote decentralized data architectures. The decentralization efforts, aimed at curbing the monopolization of data in the digital economy, promote the concept of the "*individual as the point of integration*" (MyData Global), whereby citizens can retrieve and aggregate their data from various data holders, self-hosting it in a location under their control.

Herein, it is critical to note that what is being reclaimed are copies of the data that citizens produced on an array of platforms. Given the replicability of data (Sadowski, 2019), labelling such retrieval as repossession is problematic because the original data, produced through the dispossessive datafication practices, remains with the data collectors; this, however, does not refrain these entities to refer to such interventions as data repossession.

In this regard, entities offering personal data management and exchange solutions facilitate citizens in retrieving copies of their data by either directly providing citizens with a personal data home – a cloud storage space – to host their data or offer compatibility with other independent personal cloud storage services. Citizens are thus able to connect to various accounts and import the data that has been produced therein: "*watch your social, financial, health, entertainment and wearable data stream in*" (DigiMe).

These so-called repossession efforts that enable citizens to gather their data are premised on the claim that it forms a more accurate and comprehensive data profile about them. They do not intervene in the dispossessing datafication processes but rather, following the political rationality of data as a value-adding resource, allow citizens to gain access to and potentially enable *additional* self-determined uses of their data. These entities highlight that allowing citizens to reclaim their data empowers them to avoid vendor lock-in and not be held hostage to certain platforms: *"Because applications are decoupled from the data they produce, users will be able to avoid vendor lock-in, seamlessly switching between apps and personal data storage servers, without losing any data or social connections"* (Solid). Hence, reclaiming data copies allows citizens to take them to whichever platforms and services they deem to be delivering the most value.

2.5.1.3. Action 3: Democratizing the surplus

Many of the examined entities claim to intervene in the monopolization of the value extraction efforts of major platforms by generating additional surplus for citizens through the retrieved copies of their data.

> *"[Meeco's] vision is born from a desire for disruptive anarchy; we want to change the status quo in order to create new forms of equity. We do not accept the premise that individual's information can or should be traded without their involvement or reward."*

Several entities envision and provide avenues for citizens to extract personalized benefits from the enriched datasets they hold in their personal data spaces. Whereas the citizens contribute with their personal data, these platforms provide the analytical capabilities to generate value-adding insights. Some of these entities such as DigiMe, CitizenMe, MiData and Meeco also play a fiduciary role to facilitate the citizens' data exchanges with various service providers through their platforms, ensuring that the recipients of the data do not abuse their access.

The personalized benefits include insights that help citizens' life management, such as to "*visualize all your bank operations and verify expenses*" (Cozy Cloud), "*enhance your personal and business productivity*" (Inrupt), "*improve one's self-knowledge, evaluate past decisions, make better and more informed choices*" (MesoInfos), access public services and debt relief (MyDex) as well as health-related insights to improve their quality of life (Data for Good, MiData, HIE of One).

Citizens are also afforded the opportunity to contribute their data to support market innovations and socially beneficial projects. Many entities connect citizens with data requesters such as businesses and researchers to influence innovations: they "*help those who sell ideas and products get it right more often or break some ground by taking part in medical research*" (CitizenMe) as well as "*actively contribute to medical research and to clinical trials by providing access to sets of their personal data*" (MiData), such as the Ally Science project for "*improving early warning systems and treatments for pollen allergey sufferers*" (MiData). Additionally, certain entities – such as Datangoo and CitizenMe – provide citizens with avenues to promote data donations to various charities of their choosing.

> *"We offer you the possibility of becoming a donor of those causes with which you most identify yourself, in exchange for responding to a series of questions or doing a small task, always from your mobile or computer."* (Datangoo)

Some entities critique the major platforms' and data brokers' value capture of citizens' data and seek to "*enable you to earn money by selling your data*" (PDATA). Highlighting the multi-billion-dollar data economy, they valorize the role of the citizens as producers of a valuable resource and promote financial compensation for data exchange as the way to solve the asymmetry in the data economy: they seek to "*give you the tools to help you sell your data*" (Datacoup).

These contributions are premised on the aggregation of high volumes of data to enhance the level of surplus that can be extracted from it. Given that data colonialism is driven through constant data extraction (Thatcher et al., 2016), the generation of surplus irrevocably creates a paradoxical dependency on the constant flow of data produced through the dispossessing datafication practices of corporations they seek to challenge. Although some entities – such as Datangoo, CitizenMe, and Savvy Cooperative – encourage additional production of data on their own platform, overwhelmingly, such practices engender a significant dependency on continuously retrieving copies of data primarily produced through dispossession by corporations.

2.5.2. Strategy 2: Resistance through denaturalizing and politicizing datafication – Countering the information asymmetries

As noted, corporations' data extractivism and dispossessive accumulation remains largely unchallenged due to their ability to naturalize exploitative datafication practices through obscuring them. To redress this, some of the activists we examined seek to denaturalize and politicize the datafication processes by lifting the veil of obscurity from them and offering citizens visibility over the digital traces they leave behind.

2.5.2.1. Action 4: Educating to expose exploitation in data industry

Several entities problematize the incessant capture of citizens' online engagements by educating them about the workings of the data industry. The Data Detox Kit offers a range of courses and workshops where "*through discussions and hands-on application, participants are introduced to the data collection industry and take concrete steps to live a more private life online*". Such educational tools seek to raise informed citizens who are individually aware of the exploitation they are subjected to.

Additionally, as corporations legitimize their dispossessing data accumulation and unethical uses through publishing obtuse privacy policies, certain entities seek to educate citizens by reviewing these documents and disseminating "*information about how some of the "globally prevailing tracking companies" handle our data based on their privacy policies*" (Trackography). The initiative Terms of Service; Didn't Read also intervenes towards this end by rating the privacy policies of various online platforms on various topics such as how they use citizens' information, how much control the citizens can exert over it, and the types of surveillance mechanisms employed, among others.

> "*We are a user rights initiative to rate and label website terms & privacy policies, from very good Class A to very bad Class E. Terms of service are often too long to read, but it's important to understand what's in them. Your rights online depend on them*" (Terms of Service; Didn't Read)

While these attempts do not directly challenge the dispossessive datafication of citizens, they are clearly rooted in addressing the informational asymmetries that obscure the data practices of corporations and seek to denounce and politicize them through greater awareness.

2.5.2.2. Action 5: Exposing datafication through datafication

Some of the entities we examined attempt to unveil the datafication processes citizens are subjected to by presenting to them evidence of the data they leave on digital platforms. Through the use of plug-ins and browser extensions, some entities encourage digital citizens to continue their online engagements while recording the data that is left behind. They, then, inform citizens about these digital traces, "*allow[ing] them to remain aware of who they shared information with and what information each website has compiled about them*" (Privowny), as well as "*where our data travels to when we access websites*" (Trackography), including the countries that host the servers of these websites and tracking companies. Similarly, by analyzing their digital traces, Who Targets Me captures the various advertisements that citizens are exposed to on Facebook and explicates to them the reasons for why they were targeted by particular political campaigns.

In addition to creating visibility at the individual level, these entities also engage other social actors to expose the opacity of platforms at a societal level. Through data mobility, citizens' digital traces captured by these entities are also posited as knowledge commons, which are shared with an array of stakeholders such as researchers, academics, and lawyers, among others. Whereas these actors analyze the gathered data to expose the practices of digital platforms, they also collaborate with journalists to raise social cognizance regarding the data industry and politicize the once naturalized data processes to possibly exert public pressure on the major platforms. Hence, the online engagement of citizens provides researchers and activists with the resources, namely access to their data, they would not have otherwise from which they generate visibility regarding the data industry and politicize the corporate accumulation of data at a societal level.

> *"The data collected through Trackography is open and can serve as a resource for researchers, lawyers, activists, advocates, campaigners and digital security trainers who are interested in raising critical questions about third party trackers or who want to show what happens to our data online"* (Trackography)

2.5.3. Strategy 3: Resistance through sheltering from data extraction

Some of the entities we examine provide a distinct avenue for citizens to protect themselves from data extraction by offering privacy-oriented platforms as well as promoting tools to circumvent data extraction.

2.5.3.1. Action 6: Avoidance of data capture in service delivery

Certain alternative service providers such as StartMail emailing service and Tresorit file storage provide safe spaces for citizens' information by not instrumentalizing or exposing it to anyone. They provide high-level encryption services and commit to zero-knowledge privacy, which "*means that no one, not even Tresorit, can look into the content of your files*" (Tresorit). Similarly, while Snips, a personalized voice assistant solution, allows citizens to train the assistant by answering questions to "*shar*e *your own intents simply by giving a few examples*", the generated data is stored offline on citizens' device rather than in the online environment.

The diaspora* social network serves as an effective platform for isolation from the currents of data colonialism due to its focus on decentralized data hosting, where the citizens' data that is produced is directly stored in a location of their choosing. As the platform does not have a centralized server where they can access their users' data, they cannot instrumentalize it for their benefit: "*In diaspora* you own your data. You don't sign over rights to a corporation or other interest who could use it*". Differing from the 'reclaiming data, reclaiming capital' action item we described earlier, diaspora*'s decentralized data architecture is an instantiation of *sheltering from* dispossessive datafication practices because the produced data is never in the possession of the platform; it is not a post-datafication intervention. Akin to diaspora*, alongside retrieving already existing data, certain entities – such as Solid, Inrupt and MyDex – present their future vision of creating ecosystems where citizens' personal data homes can directly receive the data that organizations generate about them to counter dispossession.

2.5.3.2. Action 7: Buttressing the defenses - Promoting tools for data circumvention

A few entities also enable citizens to proactively circumvent datafication while continuing their online engagements. For example, Data Ethics EU provides guidelines to citizens about not exposing their personal information – such as social security number, health information, and travel plans. It also provides them with a list of alternatives services that offer greater data circumvention – such as alternative search engines, browsers, maps, language translators, communication platforms, and fitness self-trackers – to avoid targeted advertising and pricing by "*smart thieves*", who base their offering on citizens' digital footprints. Privowny offers its users an array of tools like the Tracker Manager and Alias Manager which respectively block third-party trackers and advertisers on websites, as well as generate anonymized email addresses so that citizens "*don't need to disclose [their] real identity"* when registering on websites. While these methods don't offer complete protection from datafication, they are rooted in the logic of providing some circumvention from the dispossessing data extraction citizens are subjected to.

"The smart thieves are out there, and the same are insurance companies, so do not write on your 'doorstep' that you're not home" (Data Ethics EU).

2.6. Discussion

Thus far, we have examined the organization of resistance in response to the dispossessing data extraction practices in the digital realm by an array of self-described resistance entities. We highlight that these actors seek to counter the corporate accumulation of citizens' data through three main strategies: through breaking enclosures and challenging the data monopolies, through denaturalizing and politicizing datafication, and through sheltering citizens from dispossessive data extraction. In benefitting from exploring resistance against corporate accumulation in the less explored digital realm, these findings offer insights about the dual nature, the Janus duplicity, of resistance to data extractivism, related to its scope and locus, that we deem important to be highlighted. We capture our main discussion points in Table 2.3 – The Janus face of resistance to data extractivism.

2.6.1. Scope of resistance: Intervention in data colonialism

As noted, resistance is often seen to be contradictory in its very nature as it can reproduce and strengthen the dominant regimes in place (Baikovich et al., 2021; Contu, 2008; Mumby et al., 2017). In situating the strategies of the examined entities, we shed light on how resisting datafication through breaking enclosures and challenging data monopolies, as well as denaturalizing datafication were reliant upon the very data that is produced through dispossession. A dual process unfolds here. Whereas the former offered a more complicit resistance whereby the dispossessive data production was unchallenged, the latter sought to denaturalize and politicize such datafication by exposing and politicizing the surveillance mechanisms embedded in data capture. However, these affordances were made possible through the very processes that were problematized by these entities, leading to an entrenched dependency on such production processes.

Prior work on alternative organizing and resistance has highlighted how challenges to the dominant regimes require resources which are produced in them (Gibson-Graham, 1996; Ybema & Horvers, 2017; Zanoni et al., 2017). Our study reveals how such dependence can be cultivated simultaneously towards both maintaining the dominant systems but also to confront them in the context of extreme information asymmetry that enables data extractivism.

Table 2.3: The Janus face of resistance to data extractivism

	RESISTANCE (CONFRONTATION)	RESISTANCE (COMPLICITY)
SCOPE OF RESISTANCE: Intervention in Data extractivism	**Resistance through denaturalizing and politicizing datafication** • Challenges extractivist rationality that data merely 'exists' through education and exposure • Confronts informational asymmetries **Resistance through sheltering from data extraction** • Isolation from dispossessing data extraction	**Resistance through breaking enclosures and challenging data monopolies** • Dispossession continues: Extractivist rationality that data just 'exists' unchallenged • Nurtured self-exploitation: Political rationality of datafication being beneficial strengthened
LOCUS OF RESISTANCE: Individual versus collective nature of resistance	**Informed citizens can contribute to societal awareness by sharing 'exposed' digital footprint with stakeholders** • De-reifies extractivist rationality of data 'existing' • Can be potentially enabled by data mobility	**Individualization as locus of resistance fragments resistance** • Seduction of citizens through benefits pacifies them in dispossessive data producing roles (smart power)

The embedded and complicit nature of resistance (Baikovich et al., 2021; Contu, 2008; Mumby et al., 2017) requires consideration of the ideological work of the dominant regimes. Many of the entities that we examine unintentionally reaffirm some of the ideological work of data colonialism. To iterate, data colonialism is maintained through an extractivist rationality that naturalizes data as simply 'existing' and a political rationality that positions society as a benefactor of data extractivism (Couldry & Mejias, 2019). In our study, we highlight how personal data marketplaces valorize the reclamation of copies of citizens' data and direct them towards generating additional surplus for individuals or socially oriented projects. Such initiatives, in critiquing the lack of citizens' access to their data, are predicated upon the aforementioned rationalities, positing data as a beneficial resource without challenging the dispossessive nature of its production. As resistance involves the de-reification and interrogation of the dominant structure's logics (Mumby, 2005; Mumby et al., 2017), such complicity with their ideological work reproduces its dominance by keeping citizens in dispossessing data producing roles, even if now posited for an advantageous or enlightened reason.

On the contrary, the efforts to denaturalize and politicize the datafication processes, albeit reliant upon the very dispossessing data production processes, confront informational asymmetries and establish evidential value against the surveillance mechanisms that enable datafication. In doing so, the extractive rationality of data as simply 'existing' like other natural resources are problematized.

Additionally, in sheltering citizens from data extractivism, a relevant number of entities seek indeed to depart from the dominant logic and isolate citizens from the dispossessive accumulation of their data at the hands of corporations. Whereas data circumvention tools can reduce the level of information that is extracted by corporations, separating service delivery from datafication presents a promising avenue to break with the core of the dispossession mechanism. Following from Zanoni and colleagues (Zanoni, 2020; 2017), such practices can merit further attention to assess their prefigurative potential in relation to digital environments.

2.6.2. Locus of resistance: Individual versus collective nature of resistance

Our study also corroborates prior research on how resistance can contribute towards the depoliticization of dominant structures by valorizing individualization (Contu, 2008; Fleming, 2016; Fleming & Spicer, 2003a), which can weaken collective resistance and sustain dominant systems in place (Mumby et al., 2017). Previous studies have highlighted how individual, infra-political actions such as cynicism, derision and laughter can enable subjugated individuals to 'banally' resist their subjugation without generating organized, insurrectionary challenges to the power structures in place (Bucher et al., 2021; Fleming & Spicer, 2003b; Mumby et al., 2017; Peticca-Harris et al., 2020; Pignot, 2021). We broaden this debate by highlighting how digital strategies aimed at resisting data expropriation can contribute towards similar fragmentation of resistance.

As data is extracted from individuals at a personal level, efforts to challenge such extraction often endorse the individual as the rightful recipient and beneficiary of their data. Our analysis reveals that the post-datafication strategies of enfranchising the citizen and challenging data monopolies are entrenched in defending 'personal' data rights while abiding by the same individualistic (and liberal) principles by which collective resistance gets weakened. Hence, the citizen is valorized as an 'empowered' actor when maintaining control over and receiving surplus from their data, while the dispossessive data production remains unchallenged. Such actions are complicit with the extractivist imperative, whereby accumulative dispossession happens not through hard power but rather through 'smart power' which seduces and pleases citizens through narratives of individual empowerment and value-adding service provisioning (Couldry & Mejias, 2019; Han, 2017; Thatcher et al., 2016).

Our study enables us to advance previous accounts of individualized resistance that highlight the efforts of disgruntled employees to resist the ideological interpellations of the neoliberal workplace regimes (Fleming, 2016; Mumby et al., 2017) through infrapolitical acts and self-pacification (Bucher et al., 2021; Peticca-Harris et al., 2020; Pignot, 2021). We highlight that in the context of dispossessive datafication, resistance becomes fragmented through the repetition of the same ideological narratives of data colonialism that *valorize* individuality and *seduce* them through supposed benefits from their data. With citizens recovering some surplus from additional instrumentalization of their data, they can be kept in their individuated roles as data producers, away from becoming engaged in collective resistance which de-reifies and challenges the dispossessing datafication structures in play.

2.6.3. Blurring the boundaries between individual and collective action

While our analysis this far has revealed the complicity of the organized resistance through the fragmentation of resistance, it also contributes to an ongoing debate in resistance literature about the blurred boundaries between individual and collective action (Courpasson, 2017; Marsh & Śliwa, 2021). Problematizing Mumby and colleagues' (2017) categorization of resistance acts along a dichotomy of individual or collective and hidden or overt actions, recent studies highlight that resistance acts must pay due attention to their context, and that individual and covert actions can spur the organization of collective resistance (Courpasson, 2017).

Our analysis reveals that to denaturalize datafication and counter the informational asymmetries, various entities go well beyond educating citizens about data appropriation to exposing the digital footprint that citizens leave when interacting with various platforms. Such actions are rooted in denaturalizing and politicizing the data extractivism of corporations by creating informed, individual citizens. However, at community level, the gathered digital traces are also shared with other stakeholders – such as researchers, lawyers, and journalists – to create a societal level awareness about such dispossessive extraction. Hence, our study highlights digital traces as critical 'objects of resistance' (Taskin et al., 2022) through which both individual and collective action can be simultaneously organized. Thus, in the digital realm particularly, there can be communal value in creating individual opportunities for resistance.

The mobility of data to various social actors, who can analyze the data traces and disseminate the findings, can enable such practices of politicization. Resistance literature has highlighted the role of translocal practices of alternative organizers (Cruz et al., 2017; Daskalaki & Kokkinidis, 2017) and indigenous communities (Banerjee et al., 2021), who engage with dominant structures to acquire and exchange personnel, symbolic and material resources, in order to enact new reconfigurations. Treating data as 'objects of resistance' (Taskin et al., 2022), we highlight that in addition to members' mobility across fixed, physical spaces, the mobility of data can inspire individual resistance to construct collective resistance efforts that de-reify and politicize the dominant structure of data colonialism, protected by extreme information asymmetries.

2.6.4. Resistance against corporate and colonial accumulation by dispossession

Our study also seeks to contribute towards the postcolonial literature in organization studies which focuses on dispossessive corporate accumulation practices, and the resistance organized against them. As pointed out, these studies have largely been situated in relation to natural resources, involving local communities which resist through adopting violence (Banerjee, 2008; van Lent et al., 2021) as well as through the invocation of their vulnerability to societal and institutional actors (Varman & Al-Amoudi, 2016).

We contribute towards this stream of literature by highlighting how resistance is organized in the novel context of the digital realm against the dispossessive data accumulation practices of corporations, where dispossession occurs at the point of production (unlike natural resources), at an individual (not community) level. The extraction of data is less palpable due to the ideological work and regimes of 'smart power' (Han, 2017) that claim to extend the benefits of data appropriation to the same individual they are benefiting from. With dispossession less palpable in the digital context, we highlight those efforts to denaturalize datafication and de-reify the dominant rationality of data as merely 'existing' form a critical, primary avenue to generate effective resistance against such regimes.

Additionally, we highlight another vital difference between the dispossessive extractivism of data vis-à-vis natural resources: the replicability of data. Whereas natural resources are finite, and their reproduction is limited by temporal and spatial concerns, data is easily replicable and copies of it indeed can be made accessible to citizens. We argue that citizens gaining access to copies of their data does not constitute repossession, as the original data remains with the corporations that produced them through dispossessive extraction. Hence, by paying due attention to the contextual factors that shape resistance (Mumby et al., 2017), we highlight that data replicability can offer an obfuscating narrative to effectively repossessing the produced data.

2.6.5. Limitations and Future Research

Having exposed the main takeaways of our research, we acknowledge some of the limitations of our study. Our methodological approach, focused on the information given on the websites of the sampled initiatives, enabled us to compile an 'archive' (Zanoni et al., 2017) of the resistance efforts against dispossessive corporate accumulation of data. Future studies can broaden this scope by conducting in-depth, longitudinal case studies to expose the temporal dimension to resistance and how organizations that seek to resist datafication grapple with 'mission drift'. Furthermore, given the limitation of our sample, our findings present an initial, though not exhaustive, list of the categories of organized resistance to data extractivism. We also acknowledge our heavily Europe-based sample which limits its applicability to other geographical and institutional settings. Future studies can enhance the literature by exploring the role of organizational forms and socio-economic factors (communal culture, poverty) on how resistance against data extractivism is organized.

Lastly, we encourage the pursuit of studies that highlight the role of state actors vis-à-vis data extracting corporations. Previous studies have highlighted the complicity of the state in countering datafication (Zuboff, 2019). Future studies can problematize the relationship between data extractivist corporations and the state through adopting the lens of corporate political activity (Chenou & Radu, 2019) to assess the lobbying efforts of the former. The GDPR also serves as an intriguing context to study the level of protection that can be provided to citizens through the provision of data rights that, fundamentally, abide by the same individualistic logic and ideological work espoused by those platforms that make data dispossession the core of their business.

2.7. Concluding remarks

Resistance to corporate accumulation of data, as we reveal in our study, entails a variety of actions that serve to both strengthen and potentially erode the extant power relations based on the dispossessive datafication of citizens' online engagements. Whereas the negative externalities of digital platforms continue to garner attention, the very data production processes are a critical site of resistance in order to prevent the digital platforms from continuing to convert the private sphere into a 'social', which is ripe for appropriation. As mentioned by Couldry and Mejias, "*the practical starting-point for resistance to data colonialism is a vision that, until twenty years ago, would have been indisputable, but now, strangely, appears counterintuitive to many. This vision rejects the idea that the continuous collection of data from human beings is natural, let alone rational*" (2019, p. 346). We hope, with our study, to invite further scholarly focus in organizational studies towards this all-important battleground.

2.8. References

Baikovich, A., Wasserman, V., & Pfefferman, T. (2021). 'Evolution from the inside out': Revisiting the impact of (re) productive resistance among ultra-orthodox female entrepreneurs. *Organization Studies*, 01708406211024574.

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data and Society*. https://doi.org/10.1177/2053951719885967

Banerjee, S. B. (2008). Necrocapitalism. *Organization Studies*, *29*(12), 1541–1563.

Banerjee, S. B., Maher, R., & Krämer, R. (2021). Resistance is fertile: Toward a political ecology of translocal resistance. *Organization*, 1350508421995742.

Bucher, E. L., Schou, P. K., & Waldkirch, M. (2021). Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy. *Organization*, *28*(1), 44–67.

Chenou, J. M., & Radu, R. (2019). The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business and Society*. https://doi.org/10.1177/0007650317717720

Contu, A. (2008). Decaf Resistance: On Misbehavior, Cynicism, and Desire in Liberal Workplaces. *Management Communication Quarterly*, *21*(3), 364–379. https://doi.org/10.1177/0893318907310941

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349.

Courpasson, D. (2017). Beyond the Hidden/Public Resistance Divide: How Bloggers Defeated a Big Company. *Organization Studies*, *38*(9), 1277–1302. https://doi.org/10.1177/0170840616685363

Courpasson, D., Dany, F., & Clegg, S. (2012). Resisters at work: Generating productive resistance in the workplace. *Organization Science*, *23*(3), 801–819.

Cruz, L. B., Alves, M. A., & Delbridge, R. (2017). Next steps in organizing alternatives to capitalism: Toward a relational research agenda: Introduction to the Special Issue. *Management (France)*, *20*(4), 322–335. https://doi.org/10.3917/MANA.204.0322

Daskalaki, M., & Kokkinidis, G. (2017). Organizing solidarity initiatives: A socio-spatial conceptualization of resistance. *Organization Studies*, *38*(9), 1303–1325.

Fleming, P. (2016). Resistance and the "post-recognition" turn in organizations. *Journal of Management Inquiry*, *25*(1), 106–110.

Fleming, P., & Spicer, A. (2003a). Working at a cynical distance: Implications for power, subjectivity and resistance. *Organization*, *10*(1), 157–179.

Fleming, P., & Spicer, A. (2003b). Working at a cynical distance: Implications for power, subjectivity and resistance. *Organization*, *10*(1), 157–179. https://doi.org/10.1177/1350508403010001376

Fleming, P., & Spicer, A. (2008). Beyond power and resistance: New approaches to organizational politics. *Management Communication Quarterly*, *21*(3), 301–309.

Foucault, M. (1978). The history of sexuality (R. Hurley, Trans.). *New York: Pantheon*.

Gibson-Graham, J. K. (1996). Queer(y)ing capitalist organization. *Organization*, *3*(4), 541–545.

Han, B.-C. (2017). *Psychopolitics: Neoliberalism and New Technologies of Power*. Verso.

Harvey, D. (2003). *The New Imperialism*. Oxford University Press.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*. https://doi.org/10.1177/1049732305276687

Jose, A., & Lee, S.-M. (2007). Environmental reporting of global corporations: A content analysis based on website disclosures. *Journal of Business Ethics*, *72*(4), 307–321.

Karppinen, K., & Puukko, O. (2020). Four Discourses of Digital Rights: Promises and Problems of Rights-Based Politics. *Journal of Information Policy*, *10*(1), 304–328. https://doi.org/10.5325/JINFOPOLI.10.1.0304

Lehtiniemi, T. (2017). Personal data spaces: An intervention in surveillance capitalism? *Surveillance and Society*. https://doi.org/10.24908/ss.v15i5.6424

Lehtiniemi, T., & Ruckenstein, M. (2019). The social imaginaries of data activism. *Big Data and Society*. https://doi.org/10.1177/2053951718821146

Marsh, D., & Śliwa, M. (2021). Making a difference through atmospheres: The Orange Alternative, laughter and the possibilities of affective resistance. *Organization Studies*, 0170840621989008.

Martí, I., & Fernández, P. (2013). The institutional work of oppression and resistance: Learning from the Holocaust. *Organization Studies*, *34*(8), 1195–1223.

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 2053951720948087. https://doi.org/10.1177/2053951720948087

Mumby, D. K. (2005). Theorizing resistance in organization studies: A dialectical approach. *Management Communication Quarterly*, *19*(1), 19–44.

Mumby, D. K., Thomas, R., Martí, I., & Seidl, D. (2017). Resistance Redux. *Organization Studies*, *38*(9), 1157–1183. https://doi.org/10.1177/0170840617717554

Pauwels, L. (2012). A Multimodal Framework for Analyzing Websites as Cultural Expressions. *Journal of Computer-Mediated Communication*, *17*(3), 247–265. https://doi.org/10.1111/J.1083-6101.2012.01572.X

Peticca-Harris, A., DeGAMA, N., & Ravishankar, M. N. (2020). Postcapitalist precarious work and those in the ‘drivers’ seat: Exploring the motivations and lived experiences of Uber drivers in Canada. *Organization*, *27*(1), 36–59.

Pignot, E. (2021). Who is pulling the strings in the platform economy? Accounting for the dark and unexpected sides of algorithmic control. *Organization*, 1350508420974523.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data and Society*, *6*(1). https://doi.org/10.1177/2053951718820549

Strauss, A., & Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. In *Handbook of qualitative research*.

Taskin, L., Courpasson, D., & Donis, C. (2022). Objectal resistance: The political role of personal objects in workers' resistance to spatial change. *Human Relations*, 00187267211067142.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990–1006. https://doi.org/10.1177/0263775816633195

van Lent, W., Islam, G., & Chowdhury, I. (2021). 'Civilized Dispossession': Corporate accumulation at the dawn of modern capitalism. *Organization Studies*, 01708406211026127.

Van den Brink, M., Benschop, Y., & Jansen, W. (2010). Transparency in academic recruitment: A problematic tool for gender equality?. Organization studies, 31(11), 1459-1483.

Varman, R., & Al-Amoudi, I. (2016). Accumulation through derealization: How corporate violence remains unchecked. *Human Relations*, *69*(10), 1909–1935.

Walker, M., Fleming, P., & Berti, M. (2021). 'You can't pick up a phone and talk to someone': How algorithms function as biopower in the gig economy. *Organization*, *28*(1), 26–43. https://doi.org/10.1177/1350508420978831

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*. https://doi.org/10.1177/0007650317718185

Wright, E. O. (2018). *How to be an Anti-capitalist for the 21st Century*.

Wurst, L. (2015). The historical archaeology of capitalist dispossession. *Capital & Class*, *39*(1), 33–49. https://doi.org/10.1177/0309816814564131

Wu, Y.-C. J., Huang, S., Kuo, L., & Wu, W.-H. (2010). Management education for sustainability: A web-based content analysis. *Academy of Management Learning & Education*, *9*(3), 520–531.

Ybema, S., & Horvers, M. (2017). Resistance through compliance: The strategic and subversive potential of frontstage and backstage resistance. Organization studies, 38(9), 1233-1251.

Zanoni, P. (2020). Prefiguring alternatives through the articulation of post-and anti-capitalistic politics: An introduction to three additional papers and a reflection. *Organization*, *27*(1), 3–16.

Zanoni, P., Contu, A., Healy, S., & Mir, R. (2017). Post-capitalistic politics in the making: The imaginary and praxis of alternative economies. In *Organization* (Vol. 24, Issue 5, pp. 575–588). SAGE Publications Sage UK: London, England.

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs.

Chapter 3. Setting the Expectations Right: Reassessing the Power of GDPR in Protecting Online Users' Privacy

3.1. Abstract

Privacy violations against online users in the digital sphere are becoming increasingly salient and concerning. In a bid to protect its citizens, the European Union (EU) has implemented what has been called a ground-breaking public data protection measure – the General Data Protection Regulation (GDPR). In this chapter, we aim to analyze the GDPR through the lens of the social contracts theory perspective of privacy to analyze its potential and limitations in protecting online users from four major privacy controversies – namely ubiquitous data collection, misuses of data, as well as the lack of transparency and accountability of data collecting and processing entities. We highlight that the GDPR indeed provisions data rights that enables the development of a dynamic view of privacy, allowing them to exert their privacy expectations during and post-datafication. Nonetheless, the regulation places self-management of privacy responsibilities on the citizens, which can foster a privacy paradox through digital resignation. We also discuss that the impact of a normative and dynamic understanding of privacy on data ownership, wherein citizens can assert their privacy expectations even in data sharing for economic and monetization purposes.

3.2. Introduction

With the growing value of data in the age of digitalization (West, 2019; Zuboff, 2019), personal data has assumed the position of a valuable resources which not only shapes organizational functioning but organizations themselves (Alaimo, 2022; The Economist, 2017). Indeed, such developments have brought about positive changes for organizational efficiency as well as for online users (Acar & Puntoni, 2016; Majchrzak et al., 2016; McAfee & Brynjolfsson, 2012). Nonetheless, the negative externalities stemming from corporate efforts to maximize data extraction must receive due attention. Given the emerging status of data as a valuable resource, corporations and online platforms are engaging in large-scale data gathering for a variety of purposes, rendering online users' personal data as a commodity to be exploited (Martin, 2015). The data gathering and processing practices of these entities have increasingly become brazenly unethical, such as collecting data through increased surveillance of users' online activities with tracking cookies, deceptive tactics for obtaining consent, and using the gathered data in a manner that challenges the autonomy of the individual (Calo, 2013; Martin, 2016b; Royakkers et al., 2018).

Resultantly, in times of enhanced digitalization where online users have reaped benefits in forms of increased customization and greater access to services, they have been subjected to severe privacy violations relating to their personal data generated from their online activities

(Doyle, 2011). Such pervasive violations have captured the attention of the media, scholars, and regulatory bodies alike (Cadwalladr & Graham-Harrison, 2018; Martin, 2016a; Martin, 2015; Wu et al., 2014), even leading to social and academic discussions regarding the potential death of privacy (Dienlin & Breuer, 2022; Kshetri & Defranco, 2020).

With alarming privacy breaches surfacing regularly, there were calls for legislative measures to guard the privacy of online users (Bowie & Jamal, 2006; Cammaerts & Mansell, 2020; Finck, 2018; Ryz & Grest, 2016). Given the increased online vulnerability of its citizens, the European Union (EU) recognized that powerful corporations and online platforms possess the ability and incentive to unethically collect, misuse and disseminate their citizens' information. Consequently, the EU Parliament, in conformance with their desire for public regulation to address privacy concerns, has passed and implemented the General Data Protection Regulation (GDPR) – a data protection legislation – which has been referred to as the 'gold standard' legislative measure for countering the datafication practices of corporations (Andrew & Baker, 2021). The regulation, which came into implementation in May 2018, seeks to empower EU citizens by granting them more control over their personal data and its manifestations, while mandating stricter rules for corporations' data collection and processing practices (European Commission, 2017). Comprised of 99 articles, it enforces a single set of rules to be applied to all European and non-European corporations interacting with EU residents in order to hold them responsible for their privacy infringements.

It is our position that such a regulatory measure serves as a crucial setting for examining issues related to the buttressing and enervation of online privacy, both in the datafication processes as well as post-datafication protection. Scholarship has also encouraged investigations into the potential of the GDPR to place positive responsibilities on corporations, which can help to overcome the privacy paradox, referring to the fact that while individuals emphasize the importance of their privacy, they readily disclose their information to corporations (Martin, 2020). The objective of this essay, hence, is to analyze the role that the GDPR can play in enabling greater protection of online users' privacy. Specifically, the question that guides our study is – *what expectations can digital users hold of the GDPR in its role of empowering them through greaterprotection of their data?*

Although the concept of privacy has been discussed from various theoretical lenses, it is our belief that, departing from the previous literature, the social contracts view of privacy – rooted in the Integrative Social Contracts Theory (ISCT) proposed by Donaldson and Dunfee

(1999) – provides the most suitable theoretical understanding of privacy in the digital sphere due to it honouring the contextual nature of privacy (Martin, 2016b). This enables the appreciation of the diversity of norms that one individual may express in information exchange relationships depending on the setting they are in, guarding against a universal approach to privacy. Consequently, we draw on the work of Kirsten Martin (2016b) on the social contract perspective of privacy – in particular on the procedural hyper-norms of informed consent, voice and exit – for analyzing the empowering potential of the GDPR.

This essay contributes to the literature by highlighting how the social contracts theory, often criticized for its lack of applicability, can be utilized to assess the efficacy of regulatory measures such as the GDPR in empowering citizens through greater privacy protection. Secondly, we highlight that while data rights empower citizens through improved consent, voice and exit, they can also foster a privacy paradox by leading to their digital resignation through promoting self-management of privacy. Furthermore, it is asserted that in the contexts of economic interactions or data monetization, citizens still maintain certain privacy expectations.

The essay proceeds as follows. We firstly review the social contracts theory before highlighting how privacy could be understood as a social contract in the information age. Afterwards, we highlight four critical controversies that have marred online users in the digital sphere – namely ubiquitous data collection, misuses of data, lack of transparency and the lack of accountability –before analyzing the various articles of the law to assess the effectiveness of the GDPR in protecting users' privacy. We, then, discuss our results and insights to buttress the growing support for a dynamic approach to online privacy as proposed by Martin (2016b), as well as to discuss potential implications for the social contracts view of privacy.

3.3. Theoretical background

3.3.1. Integrative Social Contracts Theory

Before discussing the contractarian view of privacy, we briefly present the key concepts of the social contracts theory. With its roots in political and moral philosophy, the social contracts theory was first introduced in business ethics scholarship by Thomas Donaldson, whose book *Corporations and Morality* described corporations as moral agents, that could be held accountable for their actions (Donaldson, 1982). The moral justifiability and legitimacy of corporations is to be established on the basis of a social contract formed with members of society, which places on them certain responsibilities for expected behaviours in the actions they undertake (Donaldson, 1982, 2001).

The fundamental concept of social contracts is to ensure fairness by the inclusion of all societal contractors whose interests are affected by the operations and decisions of businesses (Dunfee et al., 1999). Economic participants *must* imply consent at the macrosocial and microsocial contracts (Donaldson & Dunfee, 1994). Macrosocial contracts, which define the normative rulesfor creating microcontracts, are formed on the basis on fundamental principles that must be appealing to all rational contractors (Donaldson & Dunfee, 2000). These principles are referred to as hyper-norms and are often detectable through the convergence principle – convergence of religious, political and philosophical thoughts (Donaldson & Dunfee, 2000; Dunfee, 1991). Hyper-norms include the most basic human principles such as political freedom, security andwell-being, the right to subsistence, fidelity, etc. (Donaldson & Dunfee, 1994). Microcontracts are agreements and collective understandings, specified by individuals and local communities, about moral norms specific to certain economic interactions in order to reduce moral opaqueness (Donaldson & Dunfee, 1994). Resultantly, microcontracts are formed in the moral free space generated by macrocontracts, which is defined by hyper-norms.

An extremely important aspect of the integrative social contracts theory lies in the concept of consent, which will also play a key role later in our analysis of the GDPR. Microsocial contracts are only binding when participants provide *informed* consent to them as well as possessing the right to exit from them (Donaldson & Dunfee, 1994). Coercive and deceptive measures invalidate implied consent (Donaldson & Dunfee, 2000). Over the years, scholars have employed the social contracts theory to address issues related to the agribusiness industry (Burkhardt, 1986), exportation of hazardous products to lesser developed countries (Cross & Winslett, 1987), and the employment of deceptive practices in consumer research among others (Smith et al., 2009).

At a time when data capture becomes a critical activity of capitalism making privacy threats more salient in our socioeconomic space (West, 2019; Zuboff, 2019), the contractarian view of business ethics is garnering increased attention from scholars to analyze ethical implications (Martin, 2016b; Martin, 2012). Due to its inclusive nature, it is particularly suited to analyze the utilizations of online users' personal data in the digital sphere as it aims to advance balanced relationships between the user and the data collecting and processing entities.

3.3.2. Privacy as a social contract

The social contracts approach to privacy aims to foster fairness for all parties that are involved in information exchange relationships (Martin, 2012). It begins with the assumption that in order to manage the tension between restricting access to personal information and social functioning, individuals share their information discriminately with others (Martin, 2016b). For example, what a person shares with their best friend may be dissimilar to what they disclose to their boss at work. Privacy expectations, hence, should be understood as 'contextual integrity' – how individuals disclose information depends on the nature of the information, their relationships with the entities with whom it is shared, and the specific purposes for the exchange. (Doyle, 2011; Martin, 2012; Nissenbaum, 2004). The social contracts of privacy are *negotiated agreements* – microsocial contracts – about the types of behaviours and benefits individuals expect from entities when they disclose their information to them (Martin, 2012). The very legitimacy of a social contract of privacy is contingent upon its conformance to three hyper-norms – namely informed consent, voice, exit (Martin, 2016b). Members of the community must possess information about the intended uses of their data to agree to them, have an influence over how their information will be collected and processed, and have the right to terminate the contract.

Informed consent refers to the participating members of the community agreeing to enter in a social contract, while understanding its terms and conditions (Donaldson, 2001). With privacy, the agreement of an individual to share their information with a party must include his or her approval of its intended use. Without understanding how their information will be collected and the purposes for which it will be used, the individual would be giving uninformed consent, nullifying the legitimacy of the social contract (Donaldson & Dunfee, 1999; Martin, 2016b). Informed consent improves users' understanding of the purposes for which the information is collected by data collectors and guards them against privacy breaches.

Voice refers to the ability of individuals to address their problems or make efforts to change the terms of their social contracts (Hoffmann, 2006). It asserts an individual should possess the ability to have an influence over how their information is utilized (Culnan & Bies, 2003). Online users can maintain influence in objecting to certain utilization of their data due to the hyper-norm of voice, placing additional responsibility on the data receiving entities and enhancing the likelihood of a more balanced relationship with the data collecting entities.

The exit hyper-norm in a social contract of privacy dictates that individuals must maintain their right of revoking their information from the entity with whom it was shared, effectively opting out from the social contract (Martin, 2016b; Martin & Murphy, 2017). Through exit, digital users can assert their privacy expectations by terminating the social contract if they feel that the information collection and processing practices of the data collectors violate their expectations. Consequently, exit provides an avenue through which the social contract perspective of privacy protects users against sustained privacy breaches.

All elements considered, the contractarian view of privacy gives due consideration to both parties that are involved in an information exchange relationship – the disempowered digital user as well as the data collecting and processing entities. Resultantly, as expectations are developed in consideration of both stakeholders, a balanced social contract emerges which protects the digital user (Donaldson & Dunfee, 1994).

3.4. Setting a map of controversies

While several types of privacy concerns have been raised in the digital sphere, we highlight what we perceive as the four most critical issues in the ensuing disempowerment of online users – ubiquitous data collection, misuses of data, the lack of transparency and the lack of accountability – which were compiled from reviewing different scholarly articles and industry reports (Christl, 2017; Christl & Spiekermann, 2016; Martin, 2016a). Our focus on these issues presents a high-level overview of the mechanisms through which personal data has increasingly been in the hands and mercy of online platforms and corporations. Not only do they cover the issue of obtaining users' data and exploiting them through it, but it also presents how informational asymmetries and accountability have continued to foster such infringing practices.

3.4.1. Ubiquitous data collection

The rise of the internet, communicative devices and online platforms have enabled consumers to engage in a wide array of online activities, ranging from social media use and online shopping to dating websites and receiving news among others (Ahern et al., 2007; Chen & Barnes, 2007; Youn, 2009). As a result, extraordinary volumes of data are being generated in the digital domain – over 2.5 quintillion bytes of new data are estimated to be created on a daily basis, with this number expected to double every four months (Hayashi, 2014; McAfee & Brynjolfsson, 2012).

Business leaders have identified the availability of such vast volume of data as an opportunity to overcome the uncertainty that marks business environments and consequently, they are engagingin privacy-infringing surveillance practices to capture it (Wielki, 2015). Dataveillance – the use of information technologies to observe and surveil online users – is becoming a salient concern in the information age (Zuboff, 2019). The advancements in technology have facilitated online platforms in surreptitiously gathering online users' personal data, derived from their online activities, while they remain uninformed (Acquisti et al., 2015).

Online users' data is gathered from a wide array of sources, leading to more variety, which further enhances the lucrativeness of data collection (Ahmadi et al., 2016). Online behaviour can be, and is, tracked through browser cookies and activities on social media platforms (Cavoukian et al., 2013; Rainie et al., 2013). The networked sensors in smart devices also facilitate data collection from devices such as fitness trackers, virtual assistants, digital thermostats and appliances among others (Christl & Spiekermann, 2016; Ziegeldorf et al., 2014). These issues raise privacy concerns because while online platforms engage in wide-scale data gathering, users often partake in activities – both online and offline – without wanting to share their information with other entities (Martin, 2018).

Users often lack the ability to opt-out from the invasive data collection practices and are in a position where they do not have the choice to not share their data, becoming 'captive audiences' to such activities (Popescu & Baruh, 2013). While users are often subjected to data collection without their consent, in some instances, many platforms legitimize their data collection practices by obtaining consent albeit in a deceitful manner. Consent is regularly attained in a pressurized manner where users are either unable to access online services without agreeing to data collection, or the choice to opt-out of sharing data is made more difficult than opting in (Lopez, 2018; Yeh, 2017).

3.4.2. Misuses of data

For online users, the privacy concerns enabled by the enhanced levels of data collection have been exacerbated by how the collected data has been utilized. Understanding privacy as contextual integrity serves as the foundation for protecting individuals from worrisome post-datafication infringements because it guards users against misuses by highlighting that the shared data is intended only for specific parties and uses (Christl & Spiekermann, 2016; Nissenbaum, 2004).

Whereas citizens can benefit from enhanced personalization of content from the collection of their data, they can also be subjected to various treatments for which they have not consented to (Christl, 2017). For example, a study showed that with an accumulation of 300 likes, Facebook can utilize algorithms to predict personality traits of their users more accurately than their close kin (Quenqua, 2015). Similarly, Amazon – the online marketplace – can analyze the purchasing patterns of users to offer discriminatory pricing for the same item if certain users have a lower price sensitivity (Zuiderveen Borgesius & Poort, 2017). As users were unaware of such utilizations, their data was used for purposes that were beyond what was communicated to them.

Additionally, firms and online platforms have undertaken their role as a member of the supply chain of information traders (Martin, 2016a). The data they collect from the online activities of their users is provided to data aggregators, who treat users' information as a commodity without any regard for their privacy to create behavioural profiles (Martin, 2015; Wielki, 2015). The Facebook-Cambridge Analytica partnership, which garnered headlines and criticisms from across all circles, is being highlighted for its role in influencing the 2016 presidential elections 2016 in the United States by using these behavioural profiles to manipulate the voting tendencies of citizens (Persily, 2017).

Misuses of data generate negative sentiments and a lack of trust within online users as this constitutes a violation of the terms under which the data was shared (Barth et al., 2006), even leading online users to perceive such activities to be 'creepy' (Shklovski et al., 2014). In particular, the adverse reaction to information misuse is stronger for sensitive information, and when the violations are intentional (Wright & Xie, 2017).

3.4.3. Lack of transparency

The ensuing privacy violations for online users have also been enabled due to the lack of transparency measures by the entities that collect and process their data without providing adequate information regarding how the data is gathered and its subsequent uses (Drucker & Gumpert, 2007). Data collectors tend to avoid measures that enhance transparency regarding their processes, such as to allow individuals to access their personal data, contributing to the power imbalance between them and online users who remain oblivious to how their informationis utilized (Christl, 2017).

While companies have asserted their commitment to respecting their users' privacy, very few of them have issued comprehensive privacy guidelines in the past (Parsons, 2019; Pollach, 2011). Furthermore, the privacy guidelines have not been properly institutionalized in business environments, leading to variations in how organizations address privacy concerns (Pollach, 2011). This is problematic because there has been a lack of definitive measures that corporations must undertake to ensure that the privacy expectations of their users are upheld.

The readability of privacy policies, referring to how easy they are for users to read and comprehend, is a prominent concern (Drucker & Gumpert, 2007; Martin, 2016a). While privacy policies intend to communicate how the corporation utilizes their consumers' data, they are often extremely verbose and, more importantly, difficult to understand (Martin, 2018). The language employed in the privacy policies also maintains obscurity and ambiguity, using words such as 'may' or 'can' when discussing their potential utilization of users′ data (Christl & Spiekermann, 2016). The readability of privacy policies, in the age of digitalization, has further decreased which has not only diminished users' trust in corporations but also subjected users to rely on them to ensure their privacy (Martin & Murphy, 2017).

Additionally, privacy policies are also inadequate for appeasing privacy concerns because they, in most cases, do not disclose practices related to information sharing with third parties – an important facet of privacy-infringing data sharing (Cranor et al., 2014; Sunyaev et al., 2014). Furthermore, Martin (2016b) discussed that consumers often hold more stringent expectations of privacy than the privacy policies of corporations as consumers are more conscious of their privacy than these entities.

Corporate privacy policies are anchored in the principles of notice and choice, where the users should be notified about the use of their data and given a choice to opt-out (Martin & Murphy, 2017). Although these concepts appear promising in meeting the privacy expectations, they arefraught with concerning issues. Corporate notices have been found to not only be extremely time-consuming and difficult to spot, they are also misleading and not targeted towards the online users (Martin, 2016b). By burying these notifications in the dense privacy policies undercircumlocutory and tortuous language, the very purpose of notice is unrealized, and the consumers remain unaware of how their information is being collected, handled and utilized.

Corporations can adopt unethical practices in regards to users' data while claiming to have notified them, regardless of how inadequately it is done (Martin, 2016a). In respect to choice, while users are presented with conditions of agreement, in most instances they are not presented with options to continue their online activity without sharing their data. Resultantly, the power scales between corporations and online users shift heavily in favour of the former as privacy policies' readability and their opportunistic twist on notice and choice make the users hostage in assuming that their information will be ethically utilized (Popescu & Baruh, 2013).

3.4.4. Lack of accountability

Data collecting entities have continued to exhibit such privacy-infringing behaviours due to the lack of the accountability that exists in the digital sphere (Christl, 2017). For online users, remaining unaware of the misuses of their data has diminished their ability to challenge platforms such as Facebook and Google and holding them accountable for their actions (Christl & Spiekermann, 2016). As such, the existing information asymmetries linked to the lack of transparency have facilitated the lack of accountability that exists for corporations and platformsin the digital sphere.

There have been calls for governments to step in and protect their citizens from such privacy violating practices despite the inclination of online firms to favour low levels of regulation in theindustry (Bowie & Jamal, 2006; Payne & Trumbach, 2009). In the United States, prior to the California Consumer Protection Act, companies had successfully resisted regulations and instead preferred self-regulation measures such as the Fair Information Practices for data protection (Martin & Murphy, 2017). The voluntary nature of these initiatives failed to place adequate pressures on corporations' unethical informational practices and with little fear of reprimand, they grew in power by brazenly continuing their surreptitious data collection practices, at the expense of online users (Martin, 2015).

In Europe, the role of government in data protection is more amplified as they have a greater preference for public legislation rather than self-regulatory measures – by online platforms and corporations – to protect their citizens´ privacy (Martin & Murphy, 2017). Consumers, when faced with privacy violations, express a greater desire to have public regulation in place and that, in countries with stringent privacy regulations, consumers experience less infringements (Bowie & Jamal, 2006; Milberg et al., 2000; Tikkinen-Piri et al., 2018). However, the speed and complexities of technological advances have allowed organizations and online platforms to circumvent the impositions on them by legislative measures.

3.5. Analyzing GDPR through social contracts view of privacy

In the following section, we undertake the task of reading the GDPR, utilizing the lens of the three aforementioned hyper-norms, to assess how it serves to empower European online users through greater protection of their data. Additionally, we highlight some of the potential limitations of the law, which should be addressed in improving the effectiveness of the provisions made by the new regulation. Our analysis is summarized in Table 3.1.

Table 3.1: GDPR articles in relation to privacy controversies and hyper-norms

Privacy Controversies	Hyper-norms of Social Contract of Privacy			Limitations
	Consent	Voice	Exit	
Ubiquitous Data Collection	-**A7:** Requiring explicit provision of consent -A7: Not allowing pre-ticked boxes for sharing data to curb coercive consent		-**A7:** Withdrawal of consent must be as easy as granting it	- Definitional unclarity: does the ease of withdrawing from consent also include not agreeing to share data in the first place?
Misuses of Data	-**A7:** Consent must be acquired for each, specific use of data	-**A7:** Online users can choose to not share their data for certain purposes -**A13:** Additional disclosure of information when personal data is shared with third-party vendors -**A21:** Data subjects can object to certain purposes (profiling) for which data is processed		- Online users may be overburdened with self-managing their privacy online due to their cognitive and time limitations
Lack of Transparency	-**A7:** The increased and easy availability of information strengthens the status of informed consent	Online users can protest against undesirable practices due to greater availability of information -**A12:** Information must be provided in clear and intelligible form -**A13:** Additional disclosure of information when personal data is shared with third-party vendors -**A14:** Additional disclosure responsibilities when personal data is shared with third parties	-A7: Online users can choose to withdraw their consent, when made aware of unwarranted practices	-Online users engage in multiple platforms, which may present this information in different forms and under different settings due to a lack of standardization. The users may not be able to conveniently access the information due to this.
Lack of Accountability		-**A15:** Online users can access their personal data in possession of data collectors and processors -**A30:** Data controllers must keep record of all their processing activities -**A21:** Data subjects can object to certain purposes (profiling) for which data is processed	-**A7:** Online users can choose to withdraw their consent, when made aware of unwarranted practices -**A17:** Online users can request the erasure of their personal data	-The lack of human and financial resources at the data protection inspectorates are making the processing of complaints slower and more inefficient.

‘A’ stands for “Article”

3.5.1. Ubiquitous data collection

A key theme that emerges in the GDPR is to promote data minimalism, whereby only as much data is collected as needed to fulfill specified purposes and it is deleted upon serving its intended uses. Another fundamental improvement in the new regulation has revolved around the concept of consent, with Article 7 of the GDPR – *Conditions for Consent* – warranting attention (European Commssion, 2017). Firstly, the GDPR imposes on the controller "*to demonstrate that the data subject has consented to processing of his or her personal data*" (European Union, 2017). The consent must be freely and unambiguously granted by the data subject either through written, oral, or electronic means. Pre-ticked boxes and silence, referring to the absence of explicit consent, does not constitute as consent (EU, 2016). Not only does the GDPR mandate that users have "*the right to withdraw his or her consent at anytime*", but also that they must be informed of this right prior to giving their consent (European Union, 2017). To further protect the right to withdraw, GDPR explicitly states that "*it shall be as easy to withdraw as to give consent*" (European Union, 2017).

3.5.1.1. Addressing the GDPR measures through the contractarian lens

The GDPR has taken several important steps in ensuring that the social contract of privacy is upheld in information collection and processing practices by strengthening the conditions of consent. First and foremost, it guards users against privacy violations by ensuring explicit consent rather than implicit consent. Under the contractarian view, implicit consent can be derived by the participation of actors (Dunfee, 1991) or in this case, data subjects. However, in the age of digitalization and surreptitious data gathering by power-wielding online platforms and corporations, users are often unaware of the extent of data gathering that results from their online activities (Martin, 2016a; van Dijck, 2014; West, 2019; Zuboff, 2019). In line with the social contract view of privacy, by requiring explicit consent, the GDPR can guide corporations to gain *informed* consent from the data subjects.

Coercive measures invalidate the hyper-norm of consent and resultantly, the social contract itself (Donaldson & Dunfee, 2000). Having pre-ticked boxes for providing consent may lead users to agree to the terms and conditions without carefully analyzing them. Not only does this not constitute as informed consent, but it can also be viewed as a way of coercing the data subjects to share their information. In describing pre-ticked boxes as not constituting consent, the GDPR has carefully guarded the EU data subjects against this threat. Furthermore, the ability to revoke consent at any time allows online users to exercise their right to exit when they desire.

3.5.1.2. Limitations of the GDPR

While the new European regulation has taken important measures to ensure ethical data collection through fortifying consent conditions, there remain certain ambiguities that can expose online users to unwarranted data collection. Specifically, while the GDPR stresses the importance of making the withdrawal of consent as easy as its provision, it remains unclear whether the withdrawal of consent is understood as revoking previously granted consent or if it also incorporates the choice of not consenting to the data gathering in the first place. Since the imposition of GDPR, concerns have been raised about the difficulties faced by users in opting out of data sharing with online platforms in the first place. In a Bloomberg article, Bershidsky (2018) reported that while consenting to data collection on Facebook was possible through a single click, opting out of it amounted to 13 clicks, where users had to navigate through circumlocutory instructions in complex language.

Consequently, despite its extensive attention to strengthening the hyper-norm of consent, there is potential for corporations to engage in practices that nudge users towards consenting to their data's collection, simply to avoid inconvenience. Under the contractarian view of privacy, this violates the status of consent because although online users may be *informed* about data collection, they have potentially provisioned it under coercion and exploitation of their time. As such practices are against the spirit of the GDPR and its focus on ethical data handling, definitional clarity regarding the withdrawal of consent can help to strengthen the very provision of consent in the first place and protect European residents from coercive consent for data sharing. For data collecting entities, it will also provide clear guidelines regarding how they present consent forms to their users and can stifle potential opportunism in utilizing ambiguous language in the GDPR to continue unethical data gathering practices.

3.5.2. Misuses of data

The GDPR has made efforts to control the misuses of data through contextualizing the conditions for consent. As per Article 7 of the law, consent is granted separately for each intended use, which must be clearly stated to the data subject. If the processing includes multiple activities, for each activity, "*the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language*" (European Union, 2017).

Furthermore, through Article 13 – *Information to be provided where personal data are collected from the data subject* – the regulation places additional disclosure responsibilities on data collectors if they intend to share their users' data with third-party vendors such as identifying the recipients of the data (European Union, 2017). The GDPR must also be implemented by these third-party vendors or processors, and data collectors who may work with such parties must ensure that they fulfil the requirements as imposed by the regulation.

Another way in which the GDPR provides greater control to data subjects over their personal data is through Article 21 – *Right to object.* Data subjects can object to and request the cessation of the processing of their information "*for direct marketing purposes…which includes profiling*" at any time without incurring any charges (European Union, 2017). Furthermore, these rights to object must be explicitly notified to the data subjects "*clearly and separately from any other information*" at the time of data collection (European Union, 2017).

3.5.2.1. Addressing the GDPR measures through the contractarian lens

Informed consent in data processing practices has also been strengthened in the GDPR by distinguishing between different intended uses by corporations and data processors. Given the complex activities that are associated with data practices of corporations, the data collecting entities could gain consent from their users, even if they were unaware of the different ways in which it will be utilized. In line with the contextual nature of privacy, data subjects may feel comfortable sharing their information for certain activities while other uses of that information may induce a sense of privacy violation (Martin, 2012).

Comprehending privacy as a social contract entails that information is shared with others with consideration of the purpose for which it will be utilized and processed (Doyle, 2011). By necessitating the acquisition of consent for all uses of the collected data, the privacy social contract between the online users and the processing entities is strengthened as data subjects are able to have a greater voice in their data's utilization. They can influence the social contract by refusing to provide consent for specific purposes which they may deem as a violation of their privacy. Similarly, the right to object complies with the contractarian view of privacy because it empowers users to have a voice in preventing their data from being used for profiling purposes. By objecting to certain uses of their data, especially direct marketing, data subjects have a greater influence in asserting how their information will be utilized, complying with the contextual nature of privacy.

3.5.2.2. Limitations of the GDPR

Despite the promising nature of the aforementioned clauses, the GDPR may contain certain limitations that hinder its ability to overwhelmingly prevent data misuses. In strengthening the conditions of informed and discriminate consent for multiple uses as well as empowering the users with greater voice through more information and the right to object, the GDPR has placed certain responsibilities the online users in self-managing their data privacy (Obar, 2015). The contractarian view of privacy, especially in the digital age, has focused extensively on highlighting the responsibility of data collectors and processors to respect and manage the privacy expectations while members of the community assert their expectations – through the hyper-norm of voice – in the information exchange transactions (Martin, 2016b).

The measures employed in the GDPR require enhanced involvement from online users. As they engage in numerous online activities on a multitude of platforms, users can become overburdened by actively managing the conditions that reduce and eliminate the privacy-infringing misuses of their data (Obar, 2015). This can lead online users to experience greater inconvenience in managing their privacy, potentially making them more careless in inactively consenting to all data uses, which may encourage certain platforms to continue their unethical practices.

As such, while the hyper-norms of consent and voice are critical to enhancing users' control over their personal data, the policymakers must remain aware of the time and cognitive limitations of their citizens in remaining engaged to manage their privacy. Although banning certain data uses may present an option to this issue, it remains difficult to achieve and can serve to harm the innovativeness and viability of certain online platforms. However, a possible option may lie in the use of user-controlled digital identities, through which online users can control the purposes for which they allow or disallow the processing of their data across multiple platforms (Obar, 2020).

3.5.3. Lack of transparency

The GPDR has placed great emphasis on making information transparent to data subjects regarding their data's collection and transfer to third-party vendors (European Union, 2017). Article 13 states that the data subject must be provided with the identity and contact information of the data controller, the purpose for the data collection, as well as to be informed if the data is to be processed by a third-party vendor (EU, 2016). Relating to indirect data collection, referring to acquisition of data from another source, Article 14 – *Information to be* *provided where personal data have not been obtained from the data subject* – imposes additional disclosure responsibilities on data controllers (EU, 2016). Not only must the sources from which the data originated must be disclosed but the categories and the recipients of subjects' personal data should also be identified (European Union, 2017).

A concerning element about privacy policies relates to their readability and the lack of information released by corporations about data transfers to third party vendors (Sheehan, 2005). The GDPR addresses these issues by mandating data collectors to adequately inform the data subjects about such activities. Article 12 – *Transparent information, communication and modalities for the exercise of the rights of the data subject* – stresses that this communication must be conducted in a "*concise, transparent, intelligible and easily accessible form, using clear and plain language*" and can employ easily visible standardized icons (European Union, 2017).

3.5.3.1. Addressing the GDPR measures through the contractarian lens

The above measures have the potential to assuage concerns that online users have raised regarding the lack of transparency, while also strengthening the social contract of privacy through providing additional information for consent conditions. As GDPR demands explicit consent from data subjects, such information can enhance the status of informed consent and validate the social contract. Possessing access to this information can also lead consumers to exercise their rights of voice through activism against inappropriate collection and transfer of their data, as well as by objecting to undesirable practices by exiting from the contract through removal of consent. The additional demands for disclosure of information collected indirectly also highlight the contextual nature of privacy as proposed by the contractarian view. As individuals share information in a discriminant manner with different entities, indirect collection of personal data is made more visible through enhanced disclosure requirements of the source.

3.5.3.2. Limitations of the GDPR

The enhanced levels of transparency in the GDPR, along with the strengthening of informed consent, possess the power to enable improved privacy protection for online users. However, similar to the conditions for consent, the GDPR can indeed promote further self-management of privacy. Additionally, the GDPR can make these augmented transparency levels more effective by specifying, in greater detail, the level of concision, intelligibility, and easy accessibility of forms. While the level of data collection varies per each platform which makes such specification more difficult for the regulators, the vagueness and open interpretability of these terms can reduce the efficacy of the imposed transparency measures. Although the information regarding their data's handling may be accessible, they may be placed under different settings for each platform, reducing the ability of online users to conveniently access them in practice. Furthermore, the information may vary in how it is presented for each platform in terms of its layout, verbosity and the use of language. As such, certain levels of standardization – mandated forms, terms and set word limits – may potentially be more effective in helping users benefit from the improved levels of the imposed transparency measures and ably strengthen the hyper- norms of informed consent, voice and exit.

3.5.4. Lack of accountability

A key principle in the formulation of the GDPR pertains to holding data collecting and processing entities accountable for their actions, by mandating responsibilities on them to enable ethical data handling practices. While the GDPR focuses extensively on accountability mechanisms, we limit our analysis to the documentation and disclosure processes, along with the imposed penalties for violations.

Article 30 – *Records of processing activities* – enforces that data controllers must keep a recording of all their processing activities, including "*the purposes of the processing*", description of "*the categories of personal data*" they keep, as well as the details of the entities with whom they have or will share the users' data (EU, 2016). Similar measures are also mandated for data processing firms who have gained access to the personal data of European citizens. Users can enforce the accountability of entities that hold their data through Article 15 – *Right to access by the data subject* – whereby they can obtain a copy of their data and file complaints with the supervisory authority for improper data uses. Additionally, along with the right to object, Article 17 – *Right to erasure (right to be forgotten)* – further allows users to issue an accountability response for unlawful processing of their personal information by seeking the removal of their data (European Commission, 2017) in exercising their right to be forgotten if they choose to withdraw their consent – according to Article 7 – for the collection and processing of their personal information (European Union, 2017).

After receiving the request for erasure, the data collecting entity must promptly remove the subject's information from their servers (EU, 2016). In case the data is being processed by a third-party firm, the controller must, in a timely manner, notify that entity about the erasure request to cease the processing activities related to that subject's data (EU, 2016). The data collector must notify the subject once the request for erasure of the data has been completed (European Union, 2017). In an attempt to encourage compliance and hold entities accountable for their actions, the violation of GDPR articles also entails heavy penalties for data collectors and processors, amounting to a maximum value corresponding to either the higher of either €20 million or 4% of their global turnover.

3.5.4.1. Addressing the GDPR measures through the contractarian lens

According to the social contract view of privacy, information exchange relationships are embedded in the purpose of generating fair contracts between the two parties. The approach to generating fairness in the relationship is based on deliberations between the two parties – in this case, the online users and the online platforms. As such, the institutional pressure through the GDPR legislation serves as an extreme measure to ensure ethical data sharing due to the continued privacy violations by the data collecting entities. However, through the rights to access and erasure, the GDPR does strengthen the hyper-norms of voice and exit. The right to be forgotten or to revoke consent serves to enhance the social contract of privacy by providing increased voice to the data subjects over the collection and utilization of their data. They can actively guard themselves against privacy violations by choosing to have their information erased following its communicated use as well as through consent withdrawal. Furthermore, they can strengthen their right to objection (Article 21) by making their displeasure more salient for the data collectors. In case the data collecting and processing corporations are deemed to be violating the trust of data subjects through unlawful processing, exercising the right to erasure represents a response, which can communicate displeasure by the unwillingness to share their information.

The right to erasure, in essence, is a form of exit, whereby the data subjects are removing themselves – through their personal information – from the social contract. Given the emphasis on timely action from the data collectors for notifying the third-party processers as well as the subjects, the GDPR can potentially facilitate the ease with which exit can be exercised, if followed to its letter and spirit. The social contract of privacy, hence, is protected by strengthening the procedural hyper-norm of exit.

3.5.4.2. Limitations of the GDPR

Through the lens of social contracts theory, rather than accountability through punitive measures, an active relationship must ensue between online users and platforms based on agreement and understanding of the fundamental principles of ethical data sharing. However, due to the brazen privacy violations by corporations (Martin, 2016a; Wright & Xie, 2017), the relationship between the two parties is mediated through data protection agencies and EU institutions rather than a direct deliberative approach.

An issue that may hinder the effectiveness of the accountability process in the GDPR relates to the lack of financial and human resources at the data protection agencies of various countries. Consequently, while many complaints have been generated by European residents regarding unethical handling of their personal data by online platforms, the process of accountability has been rather slow (Dienlin & Breuer, 2022). As such, European countries must strengthen their data protection inspectorates to ensure the effective exercise of the hyper-norms of voice and exit, through which their citizens can be better protected.

3.6. Discussion

In this essay, we have undertaken the effort to analyze the newly institutionalized GDPR under the lens of the social contracts theory to highlight its potential and possible limitations for protecting EU citizens from the privacy concerns related to their personal data. Our research aims to contribute to the growing academic debate on online privacy and the empowerment of the digital user (Draper & Turrow, 2019; Martin, 2016b; Martin, 2020; Rhoen, 2016; Wright & Xie, 2007). Although some scholars have explored the potential shortcomings of the GDPR in ensuring privacy protection (Andrew & Baker, 2021; Schade, 2023), to our knowledge, this essay is the first detailed analysis of the GDPR in light of the normative, contractarian view of privacy. Furthermore, it is our belief that the GDPR provides a fertile context for the application of the contractarian view of privacy through the three hyper-norms proposed by Martin (2016b). The social contracts theory has often gained criticism for its lack of clear guidelines for applicability in social settings (Dunfee, 2006). We aim to counter this by demonstrating the role it can play in assessing the efficacy and strength of a landmark legal framework.

In the following section, we utilize our analysis of the GDPR under the contractarian approach to lend insights for three critical discussions that are developing in the scholarly circles (i) the value of developing a dynamic approach to comprehending privacy in the digital sphere to reduce violations against online users, as well as how regulatory efforts can reinforce the privacy paradox (ii) the importance of enabling *informed* consent as well as its inter-play with the hyper-norms of voice and exit, and (iii) understanding data ownership under the contractarian lens.

3.6.1. The need for a dynamic approach to privacy versus the privacy paradox

The previously conceived access and control views of privacy posit that individuals lose their right to privacy when their information either becomes or is made accessible to another party respectively, whereby they are deemed to have relinquished any expectations of how that information will be used and for what purposes (Martin, 2016b). In this manner, these views present a static view of privacy, where the individual is not able to assert any expectations after their information becomes accessible or is shared. Approaching privacy as a social contract guards against this static view by asserting that privacy expectations are negotiated norms and that the right to privacy of the contracting entity is not surrendered upon sharing information (Martin, 2016b). Even after data is shared, individuals will have a voice in asserting how that information can be used. This ensures that an active relationship ensues between the two parties, and that data subjects can influence and object to certain uses of their information. Resultantly, the social contract view of privacy can sustain a balanced relationship between the information sharing individuals and the data collecting parties (Donaldson & Dunfee, 1994; Martin, 2016b; Martin, 2012; Windsor, 2016).

Given that the accessibility of or sharing data does not equate to surrendering expectations of privacy, the contractarian view also places the responsibility of upholding privacy expectations on corporations post-datafication. Given the wide array of violations under data capitalism, encouraging positive responsibilities for corporations for informational use is just as critical as prevent unnecessary data capture (Martin, 2020). Under the access and control views of privacy, the responsibility of maintaining privacy is directed more towards the individual; they have to ensure that their information inaccessible if they want to assert their expectations over how it is utilized (Martin, 2016b). Resultantly, the contractarian view can ensure that the provided information is better guarded due to the additional responsibility placed on the receiving entities, attempting to resolve the power imbalance between the users and data collectors (Martin, 2016b).

Through this essay, we are able to highlight the legislative measures through which the contractarian lens of privacy can be strengthened (Martin, 2016b; Martin, 2020). Particularly, the GDPR promotes the dynamic view of privacy by enabling European residents with greater involvement in their relationship with data collecting and processing companies. They are provided with measures to exert their voice in the information exchange relationship, by exercising their rights to access their data and object to certain utilizations of their information. Furthermore, through the rights which allow them to erase their data and revoke their previously given consent, online users can effectively exit from their social contract of privacy, if they find certain practices in violation of their privacy. The improved measures for transparency in the GDPR can play a vital role in enabling online users – as well as civil society actors – to voice their concerns and exit from their social contract. This is because the informational asymmetries between online platforms and users have contributed to the latter's lack of awareness regarding the collection and utilization of their data (Christl & Spiekermann, 2016; Wielki, 2015). With more information at their disposal, online users can better engage in their information exchange relationships.

Our analysis also allows us to shed light on the privacy paradox which highlights that despite claiming to value privacy, online users' willingly share their data. As Martin (2020) explicates, the dynamic view of privacy indeed explicates the privacy paradox, because sharing information does not account for the relinquishing of privacy expectations. However, regulatory measures such as the GDPR have been posited as a positive measure to shift the responsibility of maintaining privacy expectations on corporations (Cammaerts & Mansell, 2020; Martin, 2020; Yeh, 2017). This essay, however, indicates that regulations can also contribute to the privacy paradox by fostering digital resignation, enabled through the obfuscating communication used by companies (Draper & Turrow, 2019). In placing extensive responsibilities on online users through the very availability of greater volumes of information, the GDPR has the potential to overburden online users by leading them towards privacy self-management, rendering data protection less effective.

Obar (2013) has highlighted that self-management of privacy is an illusion for most online users, who neither have the time nor the cognitive ability to effectively protect themselves from every online platform they interact with. With the number of online platforms users engage in, they may find it difficult to manage their privacy settings especially due to a lack of standardization in consent forms and notifications. As a result, as online users seek to access the services of online platforms, in being overburdened with extensive disclosure, they can resign to far-ranging data capture and uses which are disclosed but ill-understood (Draper & Turrow, 2019). In this regard, the role of external data managers can be explored in future studies to assess if it serves as a better alternative in protecting privacy than self-management (Obar, 2020). Furthermore, while the data protection inspectorates of the European Union countries must be strengthened with financial and human resources to process the rights of object and exit adequately and promptly, proactive measures by these entities to actively monitor and enforce comprehensible disclosure by online platforms would enable greater protection of privacy.

3.6.2. Informed consent and the enforcing role of voice and exit

The GDPR seeks to improve the conditions of consent for online users, by providing them with more information and by countering efforts towards uninformed and coercive consent. We, however, have highlighted that a potential definitional unclarity regarding the withdrawal of consent clause, whether withdrawal of consent also signifies refusing to consent to data sharing in the first place. As the investigation reported on Bloomberg has highlighted the increased inconvenience experienced by online users in not consenting to data collection (Bershidsky, 2018), it may lead to the obtainment of illegitimate and coercive consent as the users were nudged towards data sharing (Martin, 2016b). Lopez (2018) discusses that the notion of consent, at the moment, is a deception as users are pressurized into granting it. Hence, the GDPR can better protect online users by affirming that not consenting to information sharing should be as convenient as consenting to it.

Analyzing the GDPR in light of the contractarian view also reveals how hyper-norms can serve to enforce each other (Donaldson & Dunfee, 1999), especially in the digital age. Measures that strengthened informed consent were strongly related to the principles of voice and exit. For example, to acquire informed consent, data subjects are granted voice in determining which uses of their data they agree to and can choose to exit from the contract by revoking their consent. As coercive measures to gain consent are deemed inappropriate (Donaldson & Dunfee, 1999; Lopez, 2018), consent is truly informed when the contractors can voice their perspectives and exercise their right to exit from the social contract.

While the GDPR highlights, in adequate detail, the responsibility of data collectors and processors to obtain *informed* consent, empirical studies are needed to determine their efficacy, especially given the varied cognitive abilities of data subjects. We propose that quasi-experimental research designs (Martin, 2020) can allow researchers and regulators to gain an improved understanding how online users process consent conditions, the amount of time that they spend on such measures and how this varies in terms of different online activities and intended data uses.

3.6.3. Data ownership in data markets and economic transactions

The GDPR was formulated in response to the severe privacy violations that rendered the European citizens' data as a resource to be exploited by online platforms and corporations for their commercial benefits. There had been little regard that an individual's personal data is their property rather than an unguarded resource that could be mined and utilized without ramifications (West, 2019; Zuboff, 2019). The result of such practices had been an increase in users' perception of a lack of ownership of their data – 91% of the adults surveyed in relation to these issues reported that they had no control over their personal information online (Wielki, 2015; Wright & Xie, 2017).

The GDPR has taken several initiatives to grants users greater control over their personal data. In fortifying the consent conditions, online users in Europe can potentially exercise greater control over the dissemination and uses of their information while the improved transparency measures are meant to keep them informed of its utilizations. In holding companies accountable for mischievous data related practices, the European institutions have sought to limit the violations of their citizens' data, which is deemed to be their property. The various rights of online users listed in the GDPR – such as the rights to access, erasure and object – further buttress online users' ownership of their data. Additionally, GDPR's Article 16 – *Right to rectification* – and Article 20 – *Right to data portability* – of the GDPR allow a data subject to exert their ownership over their personal data regarding correcting its inaccuracies and in demanding its dissemination to a party of one's choice.

Thus, the social contract view of privacy implies that data ownership remains fixated towards the online user, even when they forfeit the possession of the data (Martin, 2016b). Whether an individual choose to keep all their data or share all of it with online platforms, they maintain certain rights and ownership over its utilization. Such an understanding of data ownership can also be utilized in the personal data market ecosystems, where citizens share their data for monetary or non-monetary benefits (Spiekermann et al., 2015). Though online users may choose to sell their data, using that information in ways other than what was communicated to them would constitute as a privacy violation on behalf of the purchasing party. Furthermore, the hyper-norms of voice and exit also illustrate that users maintain ownership over their data even after they share it with other entities. While the ownership of data resides with its owner, the contractarian view also caters to the sharing of such information with businesses to facilitate economic functioning through mutually beneficial agreements. Ultimately, the social contracts perspective of online privacy can serve to foster fairness in the digital ecosystem while upholding economic functioning.

3.7. Conclusion

The vast array of privacy violations at the hands of data collecting and processing entities have led to the uncheckered exploitation of online users for their personal information. At this juncture, there needs to be a greater effort – by users themselves, corporations, and governments – regarding how privacy in the digital age must be comprehended. In this essay, we have utilized the social contract approach of privacy to assess the efficacy of the EU GDPR in empowering online users through greater protection of their data. We reveal that while the EU GDPR in many ways reinforces a dynamic view of privacy and empowers citizens through greater data rights and additional responsibilities for corporations, it can also overburden citizens through self-management of privacy and reinforce a privacy paradox through digital resignation. Whereas this essay offers an initial reading of the GDPR through the social contract view of privacy, we acknowledge that our focus has remained on the letter of the law, while not accounting for how this regulation has been enforced in practice. Future studies can indeed highlight the de-coupling practices of corporations and major digital platforms to continue their unethical data practices unabated.

For corporations and online platforms, great volumes of information come with greater responsibility. In these circumstances, the social contract perspective of privacy enables them to develop a deeper understanding of the privacy expectations of online users, who have been victims of alarming breaches (Martin, 2016a; Wu et al., 2014). Despite the privacy violations that it entails, the information age provides promising avenues to positively impact business decision-making as well as to offer greater customization for consumers. The growing influence of internet and online activity in our socioeconomic sphere cannot be denied or curbed. What is critical is to ensure that a balanced social contract is maintained between the data subjects and data collectors, so that for online users, the benefits do not come at the hefty price of surrendering privacy expectations.

The GDPR has been earmarked as a revolutionary step in encouraging governments to ensure the protection of online users' personal data, with several other countries following suit in creating similar regulation for their populations (United Nations Conference on Trade and Development, 2023). Despite certain limitations, the regulation has made strides in strengthening the hyper-norms of informed consent, voice and exit to potentially curb issues related to large-scale data gathering, misuses of the collected data, as well as the lack of transparency and accountability that mar the digital sphere. To fully unleash the potential of the GDPR, the data rights strengthening these hyper-norms must be complemented with the improved understanding of the behavioural limitations of users that lead to digital resignation (Draper & Turow, 2019; Obar, 2015), as well as more proactive enforcement efforts by state agencies. Being the first major data protection regulation of its kind, the GDPR must not be understood as a panacea for the challenges of unethical data practices but rather, as a first step in reinventing a new dawn in the digital age.

3.8. References

Acar, O. A., & Puntoni, S. (2016). Customer empowerment in the digital age. In *Journal of Advertising Research*. https://doi.org/10.2501/JAR-2016-007

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*. https://doi.org/10.1126/science.aaa1465

Ahern, S., Eckles, D., Good, N., King, S., Naaman, M., & Nair, R. (2007). Over-Exposed ?

Privacy Patterns and Considerations in Online and Mobile Photo Sharing. *CHI '07 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/1240624.1240683

Ahmadi, M., Dileepan, P., & Wheatley, K. K. (2016). A SWOT analysis of big data. *Journal of Education for Business*, *91*(5), 289–294. https://doi.org/10.1080/08832323.2016.1181045

Alaimo, C. (2022). From People to Objects: The digital transformation of fields. *Organization Studies*, *43*(7). https://doi.org/10.1177/01708406211030654

Andrew, J., & Baker, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, *168*(3). https://doi.org/10.1007/s10551-019-04239-z

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *Proceedings - IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/SP.2006.32

Bershidsky, L. (2018, June 29). Here´s How Facebook and Google Dodge EU Data Rules.

Retrieved from https://www-bloomberg-com.cdn.ampproject.org/c/s/www.bloomberg.com/amp/view/articles/2018-06-29/facebook-and-google-exploit-loopholes-in-eu-s-data-privacy-rules

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the Internet: Self-regulation or government regulation? *Business Ethics Quarterly*. https://doi.org/10.5840/beq200616340

Burkhardt, J. (1986). Agribusiness ethics: Specifying the terms of the contract. *Journal of Business Ethics*, *5*(4), 333–345. https://doi.org/10.1007/BF00383101

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.

Calo, R. (2013). *Digital Market Manipulation*. *SSRN*. https://doi.org/10.2139/ssrn.2309703

Cammaerts, B., & Mansell, R. (2020). Digital Platform Policy and Regulation: Toward a Radical Democratic Turn. *International Journal of Communication*.

Cavoukian, A., Davidson, A., Felton, E., Hansen, M., Landau, S., & Slomovic, A. (2013). Privacy: Front and Center. *IEEE Security & Privacy*. https://doi.org/10.1109/msp.2012.123

Chen, Y. H., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management and Data Systems*. https://doi.org/10.1108/02635570710719034

Christl, W. (2017). How Companies Use Personal Data Against People. Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. *Cracked Labs - Institute for Critical Digital Culture*.

Christl, W., & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Retrieved from https://crackedlabs.org/en/networksofcontrol

Clarke, R. (2003). Dataveillance – 15 Years On. *Privacy Issues Forum*.

Cranor, L. F., Hoke, C., Leon, P. G., & Au, A. (2014). Are They Worth Reading? An In-Depth Analysis of Online Advertising Companies' Privacy Policies. In *TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy*.

Cross, F. B., & Winslett, B. J. (1987). "Export Death": Ethical Issues and the International Trade in Hazardous Products. *American Business Law Journal*, *25*(3), 487–521. https://doi.org/10.1111/j.1744-1714.1987.tb00513.x

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*. https://doi.org/10.1111/1540-4560.00067

Dienlin, T., & Breuer, J. (2022). Privacy Is Dead, Long Live Privacy!: Two Diverging Perspectives on Current Issues Related to Privacy. Journal of Media Psychology. https://doi.org/10.1027/1864-1105/a000357

Donaldson, T. (1982). *Corporations and morality*. Englewood Cliffs, NJ: Prentice-Hall.

Donaldson, T. (2001). Constructing a social contract for business. *Business Ethics: Critical Perspectives on Business and Management*, *1*, 209.

Donaldson, T., & Dunfee, T. W. (1994). TOWARD A UNIFIED CONCEPTION OF BUSINESS ETHICS: INTEGRATIVE SOCIAL CONTRACTS THEORY. *Academy of Management Review*, *19*(2), 252–284. https://doi.org/10.5465/AMR.1994.9410210749

Donaldson, T., & Dunfee, T. W. (1999). *Ties That Bind: A Social Contracts Approach to Business Ethics*. *Academy of Management Perspectives* (Vol. 13). https://doi.org/0875847277

Donaldson, T., & Dunfee, T. W. (2000). Precis for Ties that Bind. *Business & Society Review*, *105*(4), 436–443. https://doi.org/10.1111/0045-3609.00092

Doyle, T. (2011). Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. *The Journal of Value Inquiry*. https://doi.org/10.1007/s10790-010-9251-z

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media and Society*. https://doi.org/10.1177/1461444819833331

Drucker, S. J., & Gumpert, G. (2007). Through the looking glass: illusions of transparency and the cult of information. *Journal of Management Development*, *26*(5), 493–498. https://doi.org/10.1108/02621710710748329

Dunfee. (2006). A critical perspective of integrative social contracts theory: Recurring criticisms and next generation research topics. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-006-9016-6

Dunfee, T. (1991). Business ethics and extant social contracts. *Business Ethics Quarterly*, *1*(1), 23–51. https://doi.org/10.2307/3857591

Dunfee, T. W., Smith, N. C., & Ross, W. T. (1999). Social Contracts and Marketing Ethics. *Journal of Marketing*, *63*(3), 14–32. https://doi.org/10.1016/j.neuroimage.2005.05.033 EU. (2016). Home Page of EU GDPR. *EU GDPR Terminal*.

European Commssion. (2017). GDPR Key Changes. *EU GDPR Portal*.

Finck, M. (2018). Digital co-regulation: Designing a supranational legal framework for the platform economy. European Law Review. https://doi.org/10.2139/ssrn.2990043

Hayashi, A. M. (2014). Thriving in a Big Data World. *MIT Sloan Management Review*.

Hoffmann, E. A. (2006). Exit and Voice: Organizational Loyalty and Dispute Resolution Strategies. *Social Forces*. https://doi.org/10.1353/sof.2006.0093

Kant, I., & Gregor, M. J. (1996). Groundwork of the Metaphysics of Morals (1785). *Practical Philosophy*. https://doi.org/10.1515/9783110204551

Kshetri, N., & Defranco, J. F. (2020). Is Privacy Dead? In IT Professional (Vol. 22, Issue 5). https://doi.org/10.1109/MITP.2020.2992148

Lopez, S. R. (2018). Informing Consent Giving Control Back to the Data Subject from a Behavioral. *Journal of Intellectual Property, Information, Technology & Electronic Commerce Law*, *9*(1), 35–50.

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for Digital Transformation. MIS Quarterly, 40(2).

Martin, K. (2016a). Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop? *Information Society*, *32*(1), 51–63. https://doi.org/10.1080/01972243.2015.1107166

Martin, K. (2016b). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, *137*(3), 551–569. https://doi.org/10.1007/s10551- 015-2565-9

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, *82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*(2), 135–155. https://doi.org/10.1007/s11747-016-0495-4

Martin, K. E. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics*, *111*(4), 519–539. https://doi.org/10.1007/s10551-012-1215-8

Martin, K. E. (2015). Ethical Issues in the Big Data Industry. *MIS Quarterly Executive*, *2015*(June), 74–87. https://doi.org/1540-1960

Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. Business Ethics Quarterly, 30(1). https://doi.org/10.1017/beq.2019.24

McAfee, A., & Brynjolfsson, E. (2012). Big Data. The management revolution. *Harvard Business Review*. https://doi.org/10.1007/s12599-013-0249-5

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*. https://doi.org/10.1287/orsc.11.1.35.12567

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.* https://doi.org/10.1109/SP.2006.32

Obar, J. A. (2013). *Big Data and The Phantom Public: Walter Lippmann and the Fallacy of Data Privacy Self-Management*. *SSRN*. https://doi.org/10.2139/ssrn.2239188

Obar, J. A. (2020). Sunlight alone is not a disinfectant: Consent and the futility of opening Big Data black boxes (without assistance). In *Big Data and Society*. https://doi.org/10.1177/2053951720935615

Parsons, C. (2019). The (In)effectiveness of Voluntarily Produced Transparency Reports. *Business and Society*. https://doi.org/10.1177/0007650317717957

Payne, D., & Trumbach, C. (2009). Data Mining: Proprietary Rights, People and Proposals. *Business Ethics: A European Review*, *18*.

Persily, N. (2017). Can Democracy Survive the Internet? *Journal of Democracy*. https://doi.org/10.1353/jod.2017.0025

Pollach, I. (2011). Online privacy as a corporate social responsibility: an empirical study. *Business Ethics: A European Review*, *20*(1), 88–102. https://doi.org/10.1111/j.1467-8608.2010.01611.x

Popescu, M., & Baruh, L. (2013). Captive But Mobile: Privacy Concerns and Remedies for the Mobile Environment. *Information Society*. https://doi.org/10.1080/01972243.2013.825358

Quenqua, D. (2015). Facebook Knows You Better Than Anyone Else. *New York Times*.

Rainie, L., Kiesler, S., & Kang, R. (2013). *Anonymity, privacy, and security online*. *Pew Research Center*.

Rhoen, M. (2016). Beyond consent: improving data protection through consumer protection law. *Journal on Internet Regulation - Leiden Law School*. https://doi.org/10.14763/2016.1.404

Royakkers, L., Timmer, J., Kool, L., & van Est, R. (2018). Societal and ethical issues of digitization. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-018-9452- x

Ryz, L., & Grest, L. (2016). A new era in data protection. *Computer Fraud & Security*. https://doi.org/10.1016/S1361-3723(16)30028-8

Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR? Business Ethics Quarterly. https://doi.org/10.1017/beq.2022.30

Sheehan, K. B. (2005). In Poor Health: An Assessment of Privacy Policies at Direct-to-Consumer Web Sites. *Journal of Public Policy & Marketing*. https://doi.org/10.1509/jppm.2005.24.2.273

Shklovski, I., Mainwaring, S. D., Skúladóttir, H. H., & Borgthorsson, H. (2014). Leakiness and creepiness in app space: perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2556288.2557421

Smith, N. C., Kimmel, A. J., & Klein, J. G. (2009). Social contract theory and the ethics of deception in consumer research. *Journal of Consumer Psychology*, *19*(3), 486–496. https://doi.org/10.1016/j.jcps.2009.04.007

Spiekermann, S., Böhme, R., Acquisti, A., & Hui, K.-L. (2015). Personal data markets. *Electronic Markets*. https://doi.org/10.1007/s12525-015-0190-1

Sunyaev, A., Dehling, T., Taylor, P. L., & Mandl, K. D. (2014). Availability and quality of mobile health app privacy policies. *Journal of the American Medical Informatics Association : JAMIA*. https://doi.org/10.1136/amiajnl-2013-002605

The Economist. (2017). The world’s most valuable resource is no longer oil, but data. *The Economist*.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law and Security Review*. https://doi.org/10.1016/j.clsr.2017.05.015

United Nations Conference on Trade and Development. (2023). *Data Protection and Privacy Legislation Worldwide*. UNCTAD.

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance and Society*.

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business and Society*. https://doi.org/10.1177/0007650317718185

Wielki, J. (2015). The social and ethical challenges connected with the big data phenomenon. *Polish Journal of Management Studies*, *11*(2), 192–202. Retrieved from http://www.scopus.com/inward/record.url?eid=2-s2.0-84935088081&partnerID=40&md5=22222f72d0af8c175dee96d9ccdd9426

Windsor, D. (2016). Dynamics for Integrative Social Contracts Theory: Norm Evolution and Individual Mobility. *Journal of Business Ethics*, pp. 1–13. https://doi.org/10.1007/s10551-016-3068-z

Wright, S. A., & Xie, G.-X. (2017). Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations. *Journal of Business Ethics*. https://doi.org/10.1007/s10551-017-3553- z

Wu, X., Zhu, X., Wu, G. Q., & Ding, W. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering*. https://doi.org/10.1109/TKDE.2013.109

Yeh, C.-L. (2017). Pursuing consumer empowerment in the age of big data: A comprehensive regulatory framework for data brokers. *Telecommunications Policy*. https://doi.org/10.1016/j.telpol.2017.12.001

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks*. https://doi.org/10.1002/sec.795

Zuboff, S. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. PublicAffairs.

Zuiderveen Borgesius, F., & Poort, J. (2017). Online Price Discrimination and EU Data Privacy Law. *Journal of Consumer Policy*. https://doi.org/10.1007/s10603-017-9354-z

Chapter 4. Digital Hegemony: Uncovering the role of the state in Estonia's digitalization

4.1. Abstract

The dramatic rise of digital technologies has been associated with shaping and co-constituting organizing. However, less attention is paid to how digital technologies are themselves organized by the state-business-civil society nexus to constitute a hegemonic social order. In adopting a neo-Gramscian approach to Estonia's digitalization drive, this study investigates the dynamic interactions and hegemony-building processes in three phases through which digitalization is promoted at a societal level. Given that the role of the state is oft-neglected, we contribute to the neo-Gramscian and critical scholarship in organization studies by highlighting four modalities of state governance to naturalize and stabilize digitalization initiatives: state idealization, state passivity, state activity and state re-engagement. These posit the role of the state as both a site of persuasion as situated within the historical bloc, as well as it being a conduit for coercion, due to the alignment of interests within the historical bloc. Furthermore, in acknowledging the opaque nature of technological developments, we discuss the historical bloc's role in shaping civil society through its coercive-persuasive tactics.

4.2. Introduction

This chapter adopts a neo-Gramscian approach (Bo et al., 2019; Böhm et al., 2008; Girei, 2016; Levy et al., 2016; Levy & Egan, 2003; Levy & Scully, 2007; Moog et al., 2015; Wittneben et al., 2012) to analyze the dynamic interactions and hegemony-building processes between the state, tech elites and economic actors, as well as civil society in the development and governance of Estonia's digitalization drive, which enabled the country to successfully provision 99% of its public services online. Neo-Gramscian approaches in organization studies (OS) have largely been utilized to examine struggles between the state-business-civil society nexus in contexts such as environmental crises and international development (Bo et al., 2019; Girei, 2016; Levy & Egan, 2003; Wittneben et al., 2012). While the implications of digitalization, which refers to "*the ways in which social life is organized through and around digital technologies*" (Leonardi & Treem, 2020, p. 1605), for organizing (Alaimo & Kallinikos, 2016; Faraj & Pachidi, 2021; Leonardi & Treem, 2020) and its related ethical controversies (Flyverbom et al., 2019; Greenwood & Cox, 2022; Trittin-Ulbrich et al., 2021; Zuboff, 2015) have garnered much scholarly attention is OS, investigations relating to how such a worldview is socially manifested and naturalized by the state-business-civil society nexus remain scant.

Indeed, research on digitalization has highlighted the strong interrelations between the state and private sector tech actors relating not only to enable state surveillance and technological solutions to societal issues (Flyverbom et al., 2019; León & Rosen, 2020), but also to corporate political activities to the influence regulatory efforts (Chenou & Radu, 2019; Whelan, 2019). Nonetheless, the dynamic interactions between the state-business nexus have often been ignored, especially in the context of a societal-level digitalization effort. Recent OS scholarship relating to digitalization have called for historical and contextual unpacking of the conditions and contingencies that lead to the organization of digital technologies (Beyes et al., 2022; Hensmans, 2021). We concur with these assessments and highlight that a neo-Gramscian approach to digitalization initiatives can offer a perfect avenue to investigate the hegemony-building processes which naturalize the organization of digitalization. Inspired by understanding the spread of digitalization at a societal level, our study is driven by the following questions: *what role do state-business-civil society actors play in promoting digitalization within society? How does this nexus shape the desires of the masses and limit contestations in relation to digitalization?*

In adopting a historical case study methodology to investigate Estonia's digitalization, we contribute to scholarship by highlighting the governing role of the state vis-à-vis non-state actors in organizing the hegemony of digitalization. Specifically, we contribute with a theoretical model, which captures four dynamic governing roles of the state – state idealization, state passivity, state activity, and state re-engagement – through which it serves both as a site of persuasion by the tech elites and as a conduit for persuasion and coercion towards the masses. In doing so, we enrich scholarship by highlighting the oft-neglected role of the state in both neo-Gramscian approaches and studies pertaining to digitalization in OS, which overwhelming focus on the governing roles of business and other non-state actors (Bo et al., 2019; Bucher et al., 2021; Faraj & Pachidi, 2021; Peticca-Harris et al., 2020). Additionally, we highlight how the opaque nature of technological developments facilitates the state and economic actors to limit the eventual contestations against digitalization efforts, which are pacified through coercive-persuasive tactics.

The chapter proceeds as follows. We begin by discussing the neo-Gramscian approach in OS scholarship before highlighting the hegemonic effects of digital technologies. Thereafter, the case study of Estonia's digitalization drive is introduced, and the methodology is explained. We then provide a detailed empirical section which highlights the development of Estonia's digitalization efforts by outlining its three distinct phases. This is followed by presenting our theoretical model, which highlights the governance of Estonia's digitalization, with a particular focus on the four modalities of state governance vis-à-vis non-state actors. We then conclude by highlighting the contributions of our efforts.

4.3. Theoretical background

4.3.1. The neo-Gramscian approach in organization studies

The Gramscian concept of hegemony has been employed in OS scholarship to discuss the dynamic power relations and organizational struggles between the state, corporations and civil society actors to address corporate political strategies (Levy & Egan, 2003; Levy & Scully, 2007), resistance, governance related to climate change and environmental crises (Bo et al., 2019; Böhm et al., 2008; Levy et al., 2016; Moog et al., 2015), as well as managerialism in development initiatives (Girei, 2016). In delineating the key concept of hegemony, we posit that such an approach can offer important insights relating to the governance of digitalization initiatives at a societal level.

Hegemony can be described as an "*opinion-moulding activity*" (Morton, 2007, p. 113) by social forces, which utilize coercion and consensus-building strategies to naturalize certain worldviews and posit them as being advantageous (Cox, 1999; Morton, 2007). These social forces – which include the state, actors in the economic sphere and the civil society – form a historical bloc, which acts through coercion and persuasion to establish social consensus in a bid to shape society and legitimize certain practices (Böhm et al., 2008; Gill, 2008).

Historical bloc, as per Gramsci (1971), signifies the alliances between different social groups premised upon "*the alignment of material, organizational and discursive formations which stabilize and reproduce relations of production and meaning*" (Levy & Egan, 2003, p. 806). The economic landscape and imaginaries are a critical element in the political battles for hegemony, as economic actors articulate visions and actions to lead towards particular paths (Jessop, 2010). Hegemony-building processes, hence, require careful consideration of the state-economic interactions (Levy & Egan, 2003), as they are strongly driven by '*changes in core technologies, labor processes, enterprise forms, modes of competition, and economic "identity politics"*' (Jessop, 2010, p. 346). Historical blocs are marked by contestations and persuasions within them as particular groups – especially experts – exert their influence through undertaking hegemonic projects (Girei, 2016; Joseph, 2003). These projects reflect actors' agency to direct action for specific objectives which, when aligned with the desired structural conditions of the hegemonic bloc, stabilize the proposed social order (Maielli, 2015).

To secure hegemony, however, the economic dimension has to be supported with a cultural and social imaginary which reinforces these privileges. Gramsci's key contribution emphasizes that social orders are not maintained merely through coercion but must be legitimized in the civil realm (Levy & Egan, 2003). As a result, the civil society becomes a key site where "*ruling groups organize and construct consensus, by diffusing and naturalizing certain values, worldviews and hierarchies*" (Morton, 2007, pp. 88–95). Various organizations in the civil society such as the media and educational institutions continuously conduct cultural work, positing the dominant social order being established to be the best course of action (Gramsci, 1971; Levy & Egan, 2003). However, as Gramsci (1971) highlights, the civil realm can also give rise to counter-hegemonic pressures that challenge the existing dominant structures. As a result, civil society can give rise to those political and socio-economic movements, which usher in new imaginaries.

4.3.1.1. The role of the state in constructing hegemony

Bo and colleagues (2019) have highlighted that neo-Gramscian approaches in OS scholarship, while paying due attention to economic actors and the civil society, have largely ignored the role of the state whereas Gramsci himself posited the state to be a critical actor in the organization of hegemony. This is due to two factors: (i) neo-Gramscian studies focus on the bottom-up workings, alliances, and contestations between corporations as well as civil society actors as the object of analysis (Böhm et al., 2008; Girei, 2016; Levy et al., 2016; Wittneben et al., 2012), and relatedly (ii) governments are often seen as taking a backseat to private actors in governance of various societal issues such as climate change and social responsibility due to the neoliberal ideology (de Bakker et al., 2010; Knudsen & Moon, 2017; Kourula et al., 2019).

For Gramsci, the state institutions are vital in the organization of hegemony, protecting it "by the armour of coercion" through force or legislations, as well as for preserving cohesion when conflicts and crises arise (1971, p. 263). Beyond its coercive potential, the state also has a critical role in shaping public opinions by organizing civil society, an aspect often ignored in the neo-Gramscian approaches in OS scholarship. In advancing an unpopular initiative, the state can leverage mass media and other institutions in the civil realm for ideological indoctrination to promote certain worldviews (Femia, 2011)**.** However, in interacting with the civil society, the state itself is a socially contested space, which can itself be shaped to produce different forms of state through its struggles and contestations with various civil society actors (Bo et al., 2019; Femia, 2011). As a result, at a time when the role of the state and government institutions in governance is ignored, we believe it is crucial to understand its socially constructed nature, accounting for both persuasive and coercive tactics, in advancing novel forms of organizing such as digitalization. In the next section, we highlight key insights that demonstrate how digitalization manifests itself as a hegemonic force in a bid to enrich scholarship through a neo-Gramscian lens to digitalization.

4.3.2. The hegemonic effects of digital technologies

The ubiquity of digitalization has garnered much scholarly attention, focusing on its impacts on providing affordances, its co-constitutive shaping of organizations as well as its negative implications for society (Faraj & Pachidi, 2021; Flyverbom et al., 2019; Whelan, 2019; Zuboff, 2019). There are growing calls to investigate the role of technology such as digitalization in enabling the possibility of organization, and uncovering the "*ways of thought attached to and shaped by such tools, devices and machines*" (Beyes et al., 2022; Faraj & Pachidi, 2021; Seeck et al., 2020). In this section, we highlight the critical facets in the ideology of digitalization and its hegemonic effects.

While technology shapes organizing as it "*assumes the role of the subject and governs what is proper to the subject*", it is itself organized (Beyes et al., 2022, p. 1009)**.** While the governance of digital technologies is often focused on managing the impact of such technologies (Bodrožić & Adler, 2022; Flyverbom et al., 2019), understanding how the development and organization of digitalization is governed is an intriguing task that can reveal the important role of the state, economic actors including the tech experts, as well as societal organizations. Hence, to uncover the organization of digitalization through the nexus of state-businesses-civil society, it is vital to understand the beliefs that comprise and legitimize its hegemonic effects. Critical scholarship has highlighted how technology shapes rationality and actions in capitalist societies, rooted in the normative understanding that technological progress and innovation can be the liberator of mankind by addressing social and economic shortages (Alvesson, 1985; Marcuse, 2013). The French philosopher Jacques Ellul (1964) had argued that modern societies, including states and private enterprises, are dominated by "technique", referring to hegemonic discourses around the primacy of efficiency which are especially enabled by technological innovations. Digitalization embodies a similar ideology, based on universalizing its application by reorienting problems into technological issues that can be addressed efficiently through technical solutions (León & Rosen, 2020)**.** Morozov (2013) categorizes this critical tendency as "technosolutionism", which performs a cognitive function of legitimization and necessitates social settings to be framed as domains with problems that are solvable through technological application. Given the promise of digital technologies to embody "technique", digitalization manifests itself as a hegemonic force by garnering the support of historical blocs, especially in capitalist societies.

As social progress is associated with technological innovation, critiques regarding the necessity of technology are overcome by the detachment of such developments from social relations as well as the idealization of a desired state where technological advancements are posited as benefitting individuals and society (León & Rosen, 2020). Given the complexity of technology, the development and implementation of digital tools are seen as specialized projects which often exclude citizens' involvement and public deliberation, creating a black-box mode of organizing (Pasquale, 2015). In addition to valorizing the objectivity of digital efficiency which leads to disinterest of the public, the tech elite benefits from their expertise power to create distance between their workings and the citizens, fostering conditions that universalize the application of digitalization (Alvesson, 1985; Muellerleile & Robertson, 2018). As a result, the opaque development of technological projects often escapes attention and is sheltered from contestations.

The empowered technological elite envision resistance to technological developments as a hinderance towards progress (Alvesson, 1985). As a result, possible expressions of discontent are pacified by further valorizing the technological ideology as a socially-advantageous force, especially through a culture of benefit-inducing consumption to legitimize such developments (Alvesson, 1985; Han, 2017; Trittin-Ulbrich et al., 2021). Such efforts stimulate consensus around digitalization as socially desirable and, in highlighting its development as inevitable, natural, and neutral, frame oppositional voices as illegitimate actors (Alvesson, 1985).

Recent OS scholarship relating to digitalization have called for further historical and contextual unpacking of the conditions and contingencies that lead to the organization of digital technologies (Beyes et al., 2022; Hensmans, 2021). In addition, the governing role of the state in digitalization efforts has been posited as a crucial level of analysis to assess not only the formation of such a form of organization, but also the future trajectories of digital transformations (Bodrožić & Adler, 2022). We concur with these assessments and highlight that a neo-Gramsican approach to digitalization initiatives can offer a perfect avenue to investigate such questions. Such an approach can indeed enrich scholarship on the oft-neglected state actors, particularly in the digital realm (Flyverbom et al., 2019; Kourula et al., 2019).

4.4. Methods

4.4.1. Research context

With an inductive emphasis, this chapter undertakes a qualitative, historical case study methodology to focus on the dynamic hegemony-building processes through which the main actors – the state, tech experts and the private sector, as well as the media – organized the digitalization of Estonia's public sector infrastructure. Inductive qualitative case study is a suitable methodology to theorize about the occurrence and evolution of complex phenomena (Eisenhardt, 1989), which have been utilized in neo-Gramscian studies in OS scholarship (Bo et al., 2019; Reinecke et al., 2017). However, the unfolding of these processes in relation to digitalization has largely remained undertheorized; hence, the study of Estonia's digitalization drive provides a fertile setting for such exploration.

Upon its liberation from the Soviet Union, Estonia embarked upon a journey towards adopting technology and developing a robust digital infrastructure which has enabled it to deliver all public services online with the exception of divorce and transfer of property (e-Estonia). The involvement of tech experts and economic actors in the development of the digital infrastructure, along with the acceptability of the digital services in the Estonian society, render it as an attractive setting for investigating the multiple arenas of contestations and persuasion in the hegemony-building process. The public sector is often a site of political initiatives that influence multiple arenas of society, revealing the organization of systemic and ideological power amongst various actors at a broader level (Bejerot & Hasselbladh, 2013). Consequently, our case study – given that digitalization is posited as a national branding strategy for Estonia – provides a critical instantiation of the dynamics involved in the governance of a digital regime. At a time when digitalization efforts, particularly involving public-sector initiatives such as India's Aadhaar and China's Social Credit System, receive legitimation challenges, our case study's focus on the role of the historical bloc in naturalizing Estonia's digital drive as a socially beneficial system enables visibility into the contextual and organizational processes through which digital hegemony is socially fostered.

4.4.2. Data collection

Our case study, in adopting a neo-Gramscian approach, involved collecting data primarily from interviews, which were triangulated with an array of documentary data. Additionally, field observations were conducted in the Estonian cities of Tallinn and Tartu, including visits to the e-Estonia Briefing Center – which delivers the official narrative of

Estonia’s digital journey – and the headquarters of the private-sector tech firm Cybernetica, a critical partner in the development of Estonia’s digital infrastructure.

The semi-structured interviews were conducted in two phases: 5 interviews from October 2018 to December 2018, and 26 interviews from July 2021 to November 2021. Given the small size of the Estonian population, our initial list of interviewees was complemented through snowball sampling technique; we asked our interviewees for recommendations and assistance in speaking to other relevant actors, especially the tech experts and senior government officials involved in the Estonia’s digitalization. The interviewees included 10 advisors and tech experts in the Estonian government, 2 ministers, and 3 private-sector tech experts involved in Estonia’s digitalization drive. We also interviewed 2 government spokespersons at the e-Estonia Briefing Center delivering the narrative of Estonia’s digitalization journey, 5 journalists, 8 academics as well as 1 historian. Our interviews revealed the presence of a ‘revolving door’ phenomenon between the private sector and the public sector; as such, our categorization of interviewees was based on salience of their roles during the periods of our study, from 1991 to 2007. The interviews were conducted both in-person as well as online, owing to logistical constraints and the lockdown imposed in Estonia due to a surge of cases during the Covid-19 pandemic.

Recorded with the permission of the interviewees, the interviews accounted for 39 hours of total recording time, with the average duration being 1 hour and 15 minutes. We started the interviews with a series of fixed questions regarding the motivations for and the development of Estonia’s digitalization drive, followed by the roles of various actors in the journey. Then, the interviewees were asked about the levels of contestations between the involved actors in coordinating the development of the digital infrastructure. Depending on the interviewees’ responses, a range of open questions were then posed to understand the levels of contestation and persuasion in Estonia’s digitalization drive. The interviews were conducted in English, which were then transcribed.

In addition to the interviews, we compiled a list of documentary and archival material focusing on Estonia’s digitalization, which were pre-scanned for their relevance before being scrutinized for summarization. These documents were critical in enabling us to understand Estonia’s development towards digitalization, as well as compiling a list of interviewees who were initially contacted. These documents comprise of books, news articles from the Estonian and international press, academic journal articles, reports from the Estonian government, international agencies such as United Nations and World Economic Forum, and online presentations and printed material by the Estonian government and its private sector. Our data sources are summarized in Table 1.

Table 4.1: List of data sources

Category	Data Source	Code	Number
Interview	Advisors to the state	ADV	5
	Tech experts in the government	TEG	5
	Ministers	MIN	2
	Private-sector tech experts	TEPS	3
	Government spokespersons	GOVSP	2
	Journalists	JOUR	5
	Academics	ACAD	8
	Historian	HIST	1
Document	Books	D-Book	2
	News Articles	D-NEWS	33
	Journal Articles	D-ACADART	16
	Reports	D-RPT	7
	Presentations and Printed Material	D-PPM	18

4.4.3. Data analysis

Our data analysis process involved coding the interview data, while triangulating them with the summaries and notes of the compiled documental data. Using the Atlas.ti software, we first engaged in an inductive coding strategy to identify first order codes (Strauss & Corbin, 1990) to identify the main actors as well as their activities and motivations in organizing Estonia's digitalization drive. However, in order to capture the dynamic nature of the development over time, we then categorized these first order codes in a chronological order, accounting for varied roles of the main actors involved in building and contesting Estonia's hegemonic digital drive. The chronological mapping was enabled by two processes: firstly, the documental evidence enabled us to trace the development of Estonia's digitalization; secondly, clarifications from the interviewees were actively sought during and after the interviews to ensure that the distinct phases of the development were adequately captured. This enabled us to comprehend the evolving story of Estonia's digital development over a period of 16 years, from 1991 to 2007, while remaining focused on the key critical developments.

During this process, we identified that the hegemony-building process of organizing Estonia's digitalization drive was captured in three interrelated phases, which were highlighted by most of our interviewees. The first phase related to the country's state of affairs at liberation which placed an emphasis on utilizing the affordances of technology; the second phase involved the development of the digital infrastructure, especially the back-end databases and the X-road data exchange layer; the third phase was related to the development of the e-ID card, which involved contestation from the civil society. Hence, we organized the first-order codes into the three phases, which we named 'Transition phase: Estonian liberation and visions for the future', 'Back-end Developments: Fostering the value of technology in state and society' and 'Development of the e-ID card: Universalizing digitalization'.

Through further in-depth analysis of the changing organizational processes and contestations of the main actors during these three eras, we derived 13 second-order themes to describe the hegemony-building processes in Estonia's digitalization. Then, we identified four aggregated dimensions that characterized the role of the state vis-à-vis the other actors of the historical bloc in governing the development of Estonia's digitalization. These dimensions were termed as (i) State idealization: Paving the way for technology as the liberator, (ii) State passivity: Deferring the developments to tech experts, (iii) State activity: Historical bloc's ideological indoctrination towards the masses, and (iv) State re-engagement: Facilitating the universalization of digitalization.

4.5. Findings

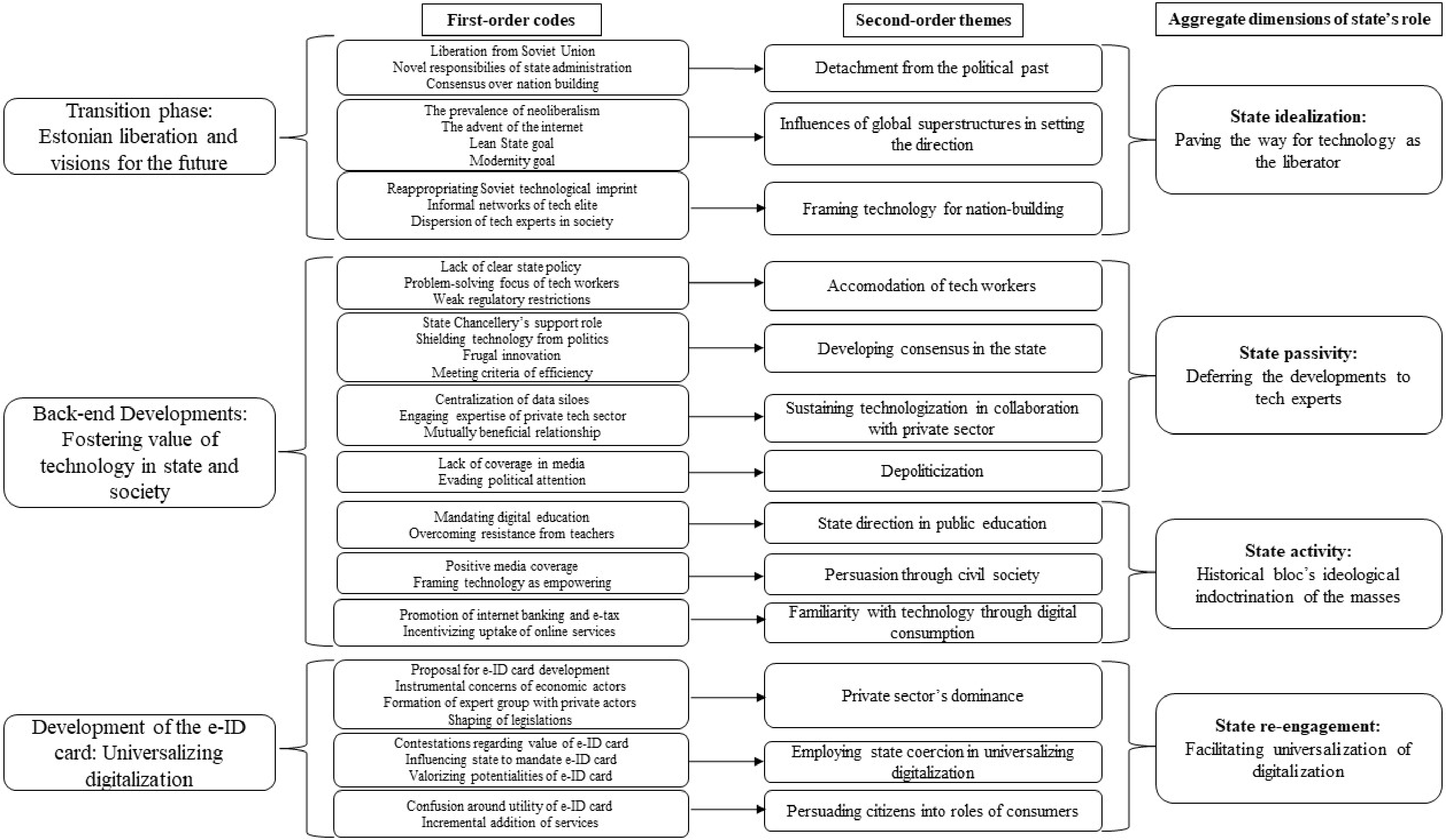
4.5.1. Transition phase: Estonian liberation and visions for the future

4.5.1.1. Detachment from the political past

On August 20, 1991, Estonia reclaimed its liberation after the 47-year Soviet rule marked by a centrally planned economy and violent suppression of Estonian culture and language (D-Book). The country's liberation from the Soviet rule brought along with it many challenges of running a country with little political experience. Due to the centrally planned economy of the Soviet Union, much of Estonia's political and administrative decision-making had been conducted in Moscow. The newly liberated Estonia sought to distance itself from the legacy of its Soviet past as it assumed new responsibilities of state administration. Having been heavily dependent on trade within the Soviet bloc, Estonia's economy collapsed upon liberation as industrial production dropped by over 30% (D-NEWS). The dire economic conditions, coupled with the country's low population of 1.55 million, brought about the type of resource scarcity which necessitated the prioritization of low-cost solutions for state administration.

> *"Politically speaking, we were liberated. From the occupation, we had a past, and we were united against this enemy. This unification was extremely valuable because it gave us a certain advantage. When we arrived to the [liberation], we had a consensus that we have to develop our country. We should reform our institutions very quickly; we should clean up all institutions from the former Communists"* (Interview - TEG)

Figure 4.1: Data structure emerging from the coding process


First-order codes
Second-order themes
Aggregate dimensions of state's role
Transition phase: Estonian liberation and visions for the future
Liberation from Soviet Union
Novel responsibilies of state administration
Consensus over nation building
Detachment from the political past
The prevalence of neoliberalism
The advent of the internet
Lean State goal
Modernity goal
Influences of global superstructures in setting the direction
Reappropriating Soviet technological imprint
Informal networks of tech elite
Dispersion of tech experts in society
Framing technology for nation-building
State idealization:
Paving the way for technology as the liberator
Back-end Developments: Fostering value of technology in state and society
Lack of clear state policy
Problem-solving focus of tech workers
Weak regulatory restrictions
Accomodation of tech workers
State Chancellery's support role
Shielding technology from politics
Frugal innovation
Meeting criteria of efficiency
Developing consensus in the state
Centralization of data siloes
Engaging expertise of private tech sector
Mutually beneficial relationship
Sustaining technologization in collaboration with private sector
Lack of coverage in media
Evading political attention
Depoliticization
State passivity:
Deferring the developments to tech experts
Mandating digital education
Overcoming resistance from teachers
State direction in public education
Positive media coverage
Framing technology as empowering
Persuasion through civil society
Promotion of internet banking and e-tax
Incentivizing uptake of online services
Familiarity with technology through digital consumption
State activity:
Historical bloc's ideological indoctrination of the masses
Development of the e-ID card: Universalizing digitalization
Proposal for e-ID card development
Instrumental concerns of economic actors
Formation of expert group with private actors
Shaping of legislations
Private sector's dominance
Contestations regarding value of e-ID card
Influencing state to mandate e-ID card
Valorizing potentialities of e-ID card
Employing state coercion in universalizing digitalization
Confusion around utility of e-ID card
Incremental addition of services
Persuading citizens into roles of consumers
State re-engagement:
Facilitating universalization of digitalization

4.5.1.2. Influences of global superstructures in setting the direction

Two major global trends – namely neoliberalism and the advent of the internet – played a critical role in shaping the vision for what the newly-liberated Estonia state would look like.

> "*Neoliberal thinking wasn't an Estonian way of doing things, but it was a coincidence. If you happen to become re-independent state in 1991, that was the international knowhow around. You wouldn't get any other advice from the West…It was also a coincidence that internet emerged around the same time. These are just two historic moments that happened at the same time when Estonia became independent*" (Interview - ACAD)

Neoliberalism – The vision for a lean government. The fall of the Soviet Union had led to a widespread belief in the "end of history" (Fukuyama, 2006) positing neoliberalism as the dominant political ideology. In alignment with the country's low resources and the desire to dispel the Soviet legacy of state domination, Estonia's political elite adopted "*one of the most radical economic liberalisation political programmes*": private sector activity was encouraged through a flat-tax rate of 20%, subsidies to industries were eliminated, and social security measures for the population were drastically cut down (D-NEWS, D-Book). The logics of neoliberalism provided the desire for the Estonian political elite to operate a lean state; this also became a vital criterion for the proliferation of digitalization in Estonia's state infrastructure.

Internet as the vehicle towards modernity. The Estonian liberation also coincided with the proliferation and optimism surrounding the revolutionary potential of the internet, which captivated the Estonian elite as a lucrative frontier for modernization and attaining global competitiveness, especially in terms of its workforce. Hendrik Ilves, who served as a foreign minister and later as the President of Estonia, recalled the opportunity of the internet in a television interview:

> "*This is one place where we are on a level playing field with everyone else. When it comes to building big highways, Germans their autobahns, the US, their interstates, they've been doing it for 60, 70 years. But here is someplace where we're no worse off than anyone else we if we get in the initial stage.*"

4.5.1.3. Framing technology for nation-building

In addition to the Soviet investments towards a high-quality education system, Estonia benefitted from the Soviet regional specialization and economic zones policy, which resulted in it becoming the hub of technological development and computer sciences. This is often reluctantly touted as "*one of the few things where the Soviet era was not completely bad*"

(Interview - JOUR). In 1960, the Institute of Cybernetics was created in Tallinn which undertook a variety of practical and research tasks such as developing microprocessors, digital and analog computers, computing languages, and software development (D-RPT). Resultantly, Estonia possessed a critical mass of people whose technological expertise was aligned to the state's ambition towards modernity and a lean state, underscoring their importance in Estonia's development.

> *"You have this small state that needs to take charge of all this stuff with little expertise and not enough manpower, so digitalization is the only option you have to make this work. Anybody who can propose something that will be a huge cost saving measure to transmit vast amounts of data instead of shipping containers of archival boxes from one city to another is going to have leverage"* (Interview - HIST)

Given the small population of the country, the Estonian tech and political elite shared close, informal networks. These networks were developed in the Soviet-rule era through their membership in the Institute of Cybernetics, as well as the Estonian Student Foundation and the Estonian Democratic Party, which were active sites for the country's liberation movement. Upon liberation, as these technological experts dispersed into academia, private sector, and the public sector, they retained close ties with each other and their colleagues in the political system. This allowed them to collaborate effectively and influence political decision makers towards digitalization from within and outside the state.

> "*I think that the change of power stirred society. People were changing positions; new positions were created both in private sector and in public sector. A lot of smart people who were worked together in the Institute of Cybernetics were suddenly spread across society, but they kept this network of relationships and this trust that they had built between their colleagues. I think that this network and trust, if you talk about e-government and how it was implemented in Estonia, this helped tremendously. Government officials, for example, were willing to take more risks because you know who's your counterpart, what they're really capable of*" (Interview – TEPS)

4.5.2. Back-end developments: Fostering the value of technology in state and society

This section highlights how the value of technology was fostered in the state and society, leading to technological developments of the public sector being deferred to the tech experts. Furthermore, the Estonian state, along with the limited civil society and economic actors, were actively involved in promoting a culture of technology to the citizens, which helped to foster a sense of digital inevitability within the masses.

4.5.2.1. Accommodation of tech workers

Tech workers who were inducted in the IT departments of various ministries were mostly involved in routine and practical tasks, such as creating and maintaining their respective databases. Rather than enacting a government-led policy, tech workers within these ministries experienced autonomy in performing their roles with a problem-solving focus.

> "*They did not have a vision. A lot of them just needed to solve problems because they were engineers. They needed to solve things like, 'we have these databases, they don't talk to each other. What do we do? It would be good for them to talk, but we don't have any money. So, we have to build something that's small, cheap', and that's what they did.*" (Interview - ACAD)

The disconnect from the Soviet bureaucratic model and the re-adoption of the 1919 constitution by the newly liberated Estonian republic also enabled tech workers to function in environments with weak regulatory restrictions and enforcement, wherein their problem-solving initiatives were not hindered by red tape and complex legislations. Workers within various departments would share their limited resources with each other by pooling their allotted funds to purchase and share equipment such as servers and routers. Although this was deemed to be against the law, the loosely enforced rules allowed the tech workers to sustain their initiatives.

> "*We were criticized by accountants because there was no track of our <laugh> finances and because it was common to share resources. It was extremely cheap and productive, but it was so informal that it was not really fitting to the bureaucracy…there was a state accountant office, this annual report saying that this is not correct, <laugh> but we just kept moving*" (Interview – TEG)

4.5.2.2. Developing consensus in the state

A critical actor in sustaining the technosolutionism efforts of the tech workers and garnering political support for the digitalization of Estonia's infrastructure was the State Chancellery. The State Chancellery, which operates as a supporting body under the Prime Minister, had a Department of State Information Systems, which worked with the various ministries to ensure collaboration and oversee the technological developments in the public sector. In "*convincing and negotiating within the government*", the State Chancellery served as an effective bridge to sustain the role and value of technology in a political environment through a "*step-by-step development*" approach (Interview - MIN).

> "*In government, technology is not the main driver. Technology, you can build, but how to organize very complex situation in government, there is politics, legislation, ministries, horizontal and vertical. This was a challenge. So, when I came in 1993, so we didn't have much technology, but we had like some ideas. Then, we got some political support but how to do it, nobody [in the political elite] was recommending that*" (Interview - ADV)

The scarcity of funds from the government – 1% of the government's budget was allocated for the development and maintenance of Estonia's information systems – also served as an enabling force for frugal innovation as tech workers made quick decisions to select and implement their proposals in a pragmatic manner. As the main criterion for the government was efficiency and cost-cutting, the tech workers' efforts to maintain databases and enable ministries' functioning without requiring excessive human power contributed to building consensus around the value of technology within the state.

A fundamental pillar of Estonia's digital infrastructure is the data exchange layer called X-road, which was created for the purpose of enabling secure data exchange between different government institutions. The underlying logic of this development remained rooted in the overarching rationale of efficiency, with technology enabling such a possibility. As database siloes emerged in the tech departments of various ministries, the State Chancellery realized the importance of having these systems communicate with each other in order to efficiently exchange data for their operations. However, developing a centralized system that integrated all the various databases and systems was extremely difficult due to organizational and financial constraints. Uuno Vallner, a digital architect at the State Chancellery who is often referred to as the father of X-road, created pilot projects to illustrate the use of the internet to facilitate data exchange between different government systems.

> "*We started from internal efficiencies…around the year 2000, we came to understanding that we can't build one big super database but we need to make sure that each database, wherever it belongs, needs to be interconnected. That was the way how everybody was able, if you have a right, to access other institutions' data and share your data. It was way more efficient than building a one big central database*" (Interview - ADV)

4.5.2.3. Sustaining technologization in collaboration with private sector

Whereas the idea of X-road gained traction, the Estonian private tech sector was engaged for its development. In 1997, the Institute of Cybernetics had been converted into a private organization called Cybernetica, although they still maintained close ties with the Estonian government due to their former affiliation as a government department (D-RPT) and the informal tech elite networks. The Estonian government's relationship with the private tech sector was a mutually beneficial one, as the government could secure customized solutions suited to their needs at a cheaper cost, while the private sector companies were able to procure business and utilize "*the Estonian government as a very good reference*" (Interview - TEPS) to attract further business. Given their expertise, Cybernetica constantly adjusted the Request-For-Proposal to influence the security design of X-road; the final design focused on enhancing security when data was in transit between different databases.

> "*If you were in software development in Estonia, in the 1990s, the only way for you to survive was public contracts because nothing else paid as well. Nothing else could get you that much work in one swoop and nothing gave you the kind of credibility to go to the international market…they knew the people who were operating in the public sector, because those were their friends from the Institute of Cybernetics or university days. The people at the various state institutes were also motivated to hire them because they didn't have that expertise in house and they were almost always much cheaper than buying from Hewlett Packard or from Oracle*" (Interview - HIST)

4.5.2.4. Depoliticization

Estonia's digital infrastructure – especially the X-road and the internal databases of various ministries – were back-end developments driven by the tech elite and as a result, they were largely uncovered in the media narratives. The developments were considered to be part of government's adminsitrative functioning and, due to their technical nature, were deemed to be unpressing to citizens' lives.

Furthermore, as X-road was developed in legal compliancy with the Estonian constitution, the project did not involve significant deliberations from politicians and evaded political attention. The project only faced minimal contestation from the Estonian government as it was posited by the tech elite as a way of enhancing the efficiency of data exchanging, which met the lean state criterion.

"*The reason why it's been so successful rather than popular is because a lot of it flew under the radar for a very long time. A lot of it was very technical and initially didn't concern all that many people. A lot of it, at first, was back end stuff. It was making the public sector run more efficiently internally*" (Interview – HIST)

While deferring the development of the digital infrastructure to tech experts, the Estonian state, along with the limited civil society and economic actors, were actively involved in promoting a culture of technology to the citizens, which helped to foster a sense of digital inevitability within the masses.

4.5.2.5. State direction in public education

As previously mentioned, the Estonian state had identified the internet as a critical avenue to modernize the nation and develop a skilled and competitive population in the increasingly globalized world. As a result, in February 1996, at the behest of the country's then foreign minister, Toomas Hendrik Ilves, the government launched the Tiigrihüpe (Tiger Leap, in English) initiative to develop digital skills in the Estonian population. This initiative aimed to put computers in every Estonian school and have them connected to the internet – a goal that was achieved by 2001 (D-PPM).

Although this initiative received contestation from teachers, who protested their low salaries and criticized the high costs of computers (D-Book; Interview - MIN), the Estonian state believed in the inevitability of digital technologies and worked to manage such resistance. The central government persuased municipalities by prioritizing funding to those local governments which implemented greater technologization of the classroom experience, including electronic courseware (D-PPM). The signalling from the government was clear – Estonia needed to build digital competences in the population to, proverbially, leap towards the future.

4.5.2.6. Persuasion through civil society.

Given the advent of the internet and the potentialities it was depicted to offer, the general coverage of the internet and technology in the Estonian press was limited yet marked with optimism. Technology was posited as enabling the liberation and progress of Estonians. Consequently, digital inevitability was strongly moralized to Estonian citizens, positing it as the 'way forward' for the newly-liberated country. As Ragne Kõuts-Klemm, a professor of journalism sociology at the Tartu University, expressed, "*We had in the media discourse that we do not have resources. We have only people and technology helps to use people as an advantage. This was a really clear promise in the media discourse that digital is our future and we should develop as the smartest nation and use technology in this sense. We had different voices in the media who stressed the need to move on with technology like teachers, scientists, entrepreneurs and, of course, politicians as well*"

4.5.2.7. Familiarity with technology through digital consumption.

Estonian citizens were also familiarized with the use of technology in their daily lives due to the advent of internet banking services in Estonia in 1996 (e-Estonia). The Estonian banking sector, driven by their desire to not build physical branches in a country with low-population density, had enabled citizens to conduct certain operations online, which was positively received by the masses (D-Book). Furthermore, in 2000, the Estonian Tax Board had influenced the government to utilize the internet to enable citizens to file their taxes online, the first public service delivered online, highlighting that such methods would lower the cost of operations and also increase the tax collection: "*It was like, here's the data. We can just say to people, instead of submitting us paper tax returns, go to internet and do it*" (Interview - TEG).

As the Estonian government had not yet developed the e-ID, they worked closely with the banking sector to perform the authentication of citizens: "*banks already had built the secure system. So, if we log into internet banks, we can log into the tax portal through that*" (Interview - ADV). To encourage the uptake of e-tax, the government promised quicker and higher rebates for online tax filers rather than traditional, paper-based filings. Consequently, due to such interaction with technology, Estonian citizens developed some familiarization with accessing services, public and private, through online channels.

"*If people get to use digital technologies in banking, which they might do like every day or every week, it also makes it easier for them to interact with digital tools with government or any other services that they don't use that often…in that sense, it educated people how to use those technologies*" (Interview - ADV)

4.5.3. Development of the e-ID card: Universalizing digitalization in Estonia

The final piece of the technical infrastructure that enabled the provision of digital public services was the decision by the Estonian government to develop and issue electronic identity (e-ID) cards to its citizens. In 1992, Estonians had been issued 10-year passports that were to expire in 2002. Resultantly, the government, led by the Ministry of the Interior, was interested in issuing a new identity document – an identity card – that would be more convenient for the citizens to carry. A debate started regarding inserting a chip to the ID card, which would enable citizens' identification in online environments. This proposal was not inspired by a carefully crafted vision of delivering public services but rather the techno-optimism of the tech elite, who believed it to offer unforeseen potentialities and strongly shaped its direction.

4.5.3.1. Private sector's dominance: Linking instrumental concerns with agenda of modernity

The e-ID card's development was influenced by the tech elite's ideological mutualism with the state regarding digital inevitability, as well as the instrumental concerns of banks and telecommunications companies. The Estonian banking and telecommunication sectors deeply espoused the primacy of digital technologies, seeing it as a critical factor for their future success. While Estonian banks had already launched internet banking in the country in 1996 to "*put the customers to do the labour and reduce costs for the bank*" (Interview - ACAD), their authentication and security systems were becoming obsolete. Hence, the e-ID initiative by the Estonian state would reduce the financial burden on them to launch their own digital identity solutions and place them in a better position to compete with the Scandinavian banks entering the Estonian market. For the telecommunication companies, the adoption of the e-ID card would enable them to evince the value of the internet to the citizens, resulting in opportunities to provide more internet connections (Interview - JOUR).

> "*It was hugely promoted by telecoms and banks, who were basically the forces behind the Estonian ID card. There's a very clear business logic to this, which is that in the early 2000s, Estonian banks were starting to see that Nordic banks are eyeing the market. Estonian banks had some form of tele-banking already in existence but it was woefully out of date…the idea was that if the Estonian state puts in place a system of digital authentication that the banks can all get behind, that's a huge cost saving measure for them. It opens up a whole new market for them because everybody who is now forced by law to get an Estonian ID card will now become a potential client for their specific banks, which use the same authentication system*" (Interview - TEPS)

As a result, given the prevalence of tech expertise in the private sector, "*a expert group was formed that consisted of government people, from private sector, banks, and Cybernetica*" to work on the initiative (Interview – TEPS). The e-ID card's development was marked by the tech elites becoming critical actors in shaping legislations to ensure the proliferation of the new technology. The primary functions of the e-ID card were to ensure authentication of citizens and enable signing of documents in the digital environment. As a result, the working group developed the Digital Signature Act for the Estonian government to pass, which would make digital signatures legally binding (D – PPM). Such a measure would enable the signing of documents and contracts online, allowing them to carry weight in the court of law and facilitating the use of the e-ID card for transactional purposes.

4.5.3.2. Employing state coercion in universalizing digitalization

Whereas the hitherto technical infrastructure developments related to back-end systems, they were largely depoliticized as technical projects which remained invisible to the larger populace. On the contrary, as the e-ID card was going to be delivered to the citizens, this initiative became a point of vigorous debate amongst politicians. The initiative was largely seen as being unnecessary due to the lack of a clear vision of the utilization of the chip, adding unnecessary costs for the government and the citizens who would have to pay for it.

> "*The central question was, should the ID card be compulsory for everybody? There was clear resistance to that. What's the point? Because every citizen will now need to also pay for that. There is some cost involved for everybody when they are paying for the new documents and, again, it was a new technology with maybe a lot of promise but there was no clarity about what's to come. I think probably nobody knew. They were building a platform with unknown uses and because there were costs involved to every citizen, there was skepticism, 'why are we forcing everybody to make these costs?'*" (Interview - MIN)

In face of such criticism, the tech elite influenced the Estonian government to make the ID card mandatory rather than a voluntary initiative. The Union of Estonian Information Technology and Telecommunication enterprises (ITL) wrote a letter to Prime Minister Mart, marked by the techno-optimism narratives of the potentialities of the new technology, as well as its signalling effect of promoting Estonia's image as an innovation country.

> "*We are convinced that ID card applications will not be created until there is a critical mass of card users. The latter, however, cannot be achieved with the voluntary introduction of the card…The Union recognized that making the ID card voluntary also postpones the wide-scale implementation of the digital signature law adopted by the Riigikogu [Parliament] in March of last year for an unknown period of time...Its impact on the image of the Estonian state is also important — the transition to an ID card confirms Estonia's reputation as an innovative country in other parts of the world. ITL hopes that Estonia will not miss this opportunity*" (D-NEWS)

Against the opposition, Prime Minister Mart Laar gave the go ahead for the e-ID in the final days of his government in 2002 while the criticism related to the cost of the card was managed by subsidizing its price at 150EEK (9.60 EUR) for adults, and 25 EEK (1.60 EUR) for retirees and children (D-ACADART). The banks were instrumental in the distribution of the e-ID cards: "*We sent the ID card to the closest bank office, and the bank office would make the identification process and give me the ID card"* (Interview - ADV). The economic actors' influence and instrumental concerns in promoting the e-ID card is further reflected in the fact that the generation of certificates which enabled the provision and verification of digital signature (D-RPT) was assumed by S&K ID Solutions – a identity service company partnered by the major Estonian banks and telecommunications companies (SK.ee). This served as additional motivation for these actors to expand the use of the e-ID card.

> "*We developed a business model in S&K as a validation service, not for free but a paid service. That means that we earned from every transaction made from the card because you have to check validity of the certificate when it's used. So, putting this price structure made us interested to get more and more usage*" (Interview - TEPS)

4.5.3.3. Persuading citizens into the role of consumers

The provision of the e-ID card was the first instance of large-scale public awareness of the government's technical initiatives. However, given the ideological indoctination regarding the value of technology that we alluded to earlier by the state as well as the economic and civil society actors, citizens' and politicians' contestation was largely limited towards the utility of the e-ID card. Furthermore, as the concerns around privacy and state surveillance were not active social discussions around the internet at this time, the citizens' response to the e-ID card was mainly composed of confusion and ridicule surrounding its utility.

> "*People were joking that, what is this card good for? The joke was that in the winter, ifyou have ice on your car, you can basically get the ice off with it*" (Interview - MIN)

The Estonian state and tech elite were able to influence the adoption of the e-ID card through appealing to citizens' concerns about utility and valorizing its benefits. The contestation around the e-ID card was managed by making the e-ID card ubiquitous for interacting with the private and public sector. The private sector use of the e-ID card, such as for online banking, as well as its use as a health card and a driving license helped to increase its uptake (D-PPM). In addition to e-tax, various Estonian state ministries started to incrementally add more services that were accessible digitally through the e-ID card. These included utilizing the card for bus tickets in 2003, e-voting in 2005, e-Health records in 2008 and e-Prescription (D-PPM). As a result, citizens were persuaded into their roles of 'citizens as consumers' by establishing evidential value regarding the convenience offered by the e-ID card.

"*People start to use the e-ID and nothing bad happens. Trust building takes time but trust building cannot be solved in a way that you have some big campaigns. People need to feel it*" (Interview - ADV)

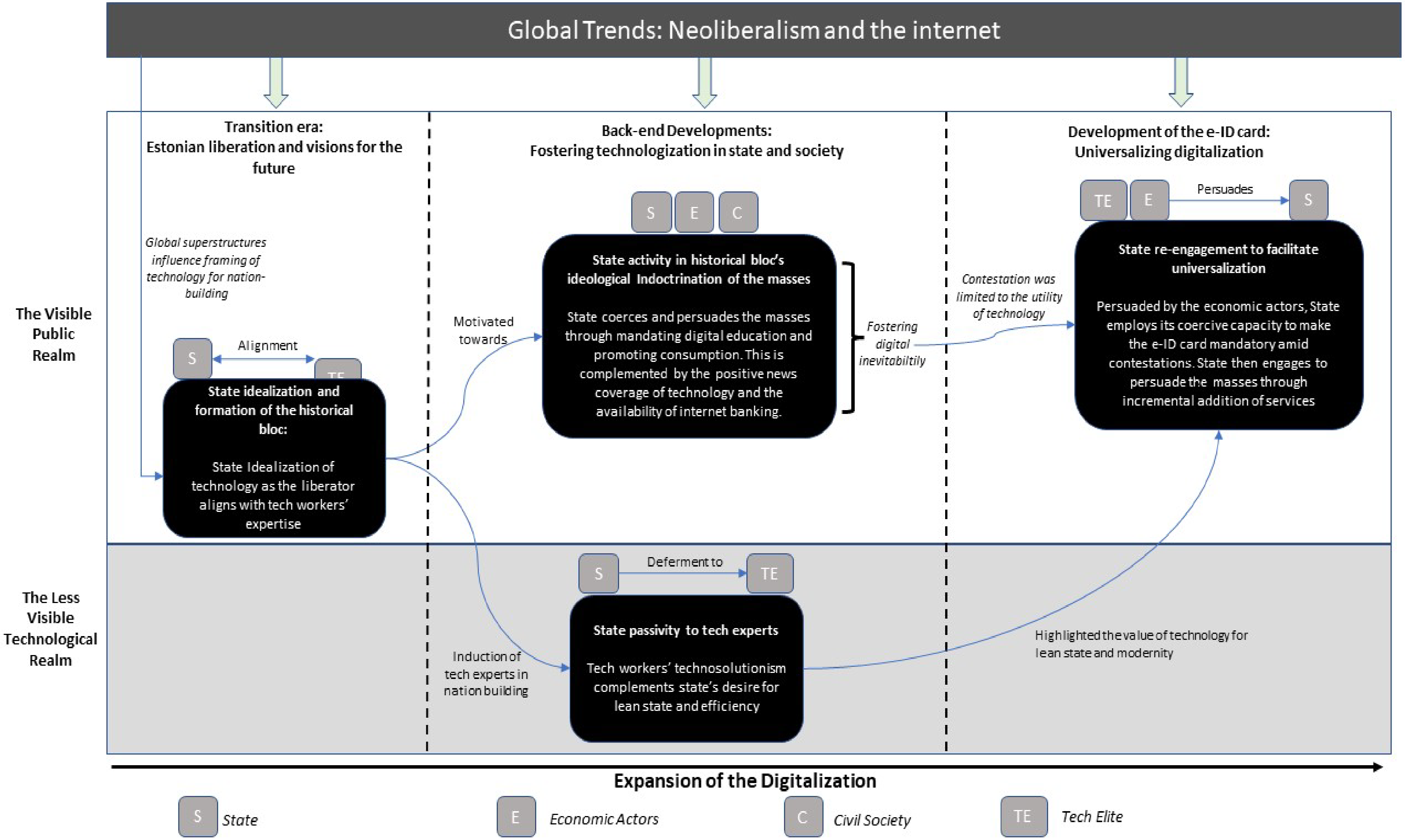
4.6. Theorizing governance in Estonia's digital hegemony

In this section, building upon our analysis, we delineate the hegemony-building processes that marked the governance of Estonia's drive towards digitalization. By governance, we do not merely refer to corporate governance strategies but rather '*to the wider concept of societal governance, that of the collective means to give "direction to society"*' (Kourula et al., 2019). In doing so, we highlight how these processes involved active negotiation and persuasion tactics within the historical bloc (Gramsci, 1971; Levy & Egan, 2003) – comprised of the state, economic actors including tech elites, and the media – as well as ideological indoctrination to mould the citizens' opinions which limited the masses' counter-hegemonic potential (Morton, 2007). This allows us to theorize four dimensions related to the dynamic role of the state in organizing digital hegemony, while also shedding light on how the opaque nature of digital developments limit contestations.

4.6.1. State idealization: Paving the way for technology as the liberator

Upon liberation from the Soviet Union, the Estonian political elites were driven by a 'desired state' of detachment from the Soviet legacy to become a modern state. The serendipitous timing of Estonia's liberation coincided with the dominance of the global superstructures of neoliberal ideology and the advent of the internet. Envisioning technology as a liberating force for the Estonian society (Alvesson, 1985; Marcuse, 2013)**,** the state developed a strong relation with the country's technologically skilled class, itself a Soviet-era imprint (Marquis & Qiao, 2020; Mees-Buss & Welch, 2019), who would go on to assume an important role in Estonian society by providing the linkage between technology and the lean state-modernization political agenda (Girei, 2016; Levy & Egan, 2003). The formation of the digital historical bloc (Levy & Egan, 2003), driven by the economic and political landscape, enabled the direction of the Estonian society towards digitalization.

Figure 4.2: Governance in Estonia's Digitalization


Global Trends: Neoliberalism and the internet
Transition era:
Estonian liberation and visions for the future
Back-end Developments:
Fostering technologization in state and society
Development of the e-ID card:
Universalizing digitalization
Global superstructures influence framing of technology for nation-building
The Visible Public Realm
S
Alignment
TE
State idealization and formation of the historical bloc:
State Idealization of technology as the liberator aligns with tech workers' expertise
Motivated towards
S
E
C
State activity in historical bloc's ideological Indoctrination of the masses
State coerces and persuades the masses through mandating digital education and promoting consumption. This is complemented by the positive news coverage of technology and the availability of internet banking.
Fostering digital inevitabiltily
Contestation was limited to the utility of technology
TE
E
Persuades
S
State re-engagement to facilitate universalization
Persuaded by the economic actors, State employs its coercive capacity to make the e-ID card mandatory amid contestations. State then engages to persuade the masses through incremental addition of services
The Less Visible Technological Realm
Induction of tech experts in nation building
S
Deferment to
TE
State passivity to tech experts
Tech workers' technosolutionism complements state's desire for lean state and efficiency
Highlighted the value of technology for lean state and modernity
Expansion of the Digitalization
S
State
E
Economic Actors
C
Civil Society
TE
Tech Elite

In concurrence with the neo-Gramscian approach, at the expense of the masses, the tech elite benefitted from the possession of those technological skills that aligned with the state's political aims to attain a privileged position (Bates, 1975; Moog et al., 2015), allowing them to direct and shape state action. The state's idealization of digital technologies also mirrors prior discussions on the ideology of technology, wherein the valorization of "technique" is considered to be the liberating force for society (Ellul, 1964; Alvesson, 1985; León & Rosen, 2020). Consequently, uncovering the hegemony-building processes enables us to draw insights about the dynamic interactions of the historical bloc actors amongst themselves as well as with the masses, which established the digital social order through persuasion and coercion tactics.

4.6.2. State passivity: Deferring the developments to tech experts

The induction of tech experts in the Estonian public sector enabled the formation of Estonia's technical infrastructure, underscored by the logics of efficiency-enhancing technosolutionism (Morozov, 2013). This phase is marked by the state's passivity towards the workings of the tech experts, leading to the development of the technological infrastructure of the Estonian state. Towards this end, the tech workers were unbounded by excessive oversight and regulatory enforcement in their technological problem-solving. The State Chancellery's Department of State Information Systems, itself composed of tech experts, also worked to protect the digitalization of the public sector from political interference and contestations. Such efforts generated momentum to create the X-road data exchange layer through the involvement of Cybernetica, which later enabled the expansion of digitalization in the citizens' realm through the provision of public services online.

From a neo-Gramscian perspective, the technologization of the public sector infrastructure highlights the role that hegemonic actors within the historical bloc, tech experts in this instance, play in shaping the very institutions they are embedded in to sustain their dominance within the state (Böhm et al., 2008; Levy & Egan, 2003). As Gramsci (1971) highlighted that the state itself must be considered as a socially contested process, the passivity adopted by the Estonian state allowed the workings of tech experts to maintain consensus within it regarding the value of technology. This is because even though the possession of funds instantiates power for the state (Girei, 2016), the hegemonic projects that established the tech experts' power in the state aligned with the structural hegemonic goals of enabling a lean, efficient state. As such, the technosolutionism of the tech experts complemented the technique-driven goals of the Estonian state (Ellul, 1964; Morozov, 2013) and led to the stability of the historical bloc, even with the state in a passive role (Joseph, 2003; Maielli, 2015).

Whereas hegemony is an unstable social order as it is open to contestation and counter-hegemonic pressures for subaltern groups, we highlight that the lack of civil society involvement in this phase, which sustained the hegemonizing efforts, pertains to the general disinterest of the masses fostered through the digital ideology (Alvesson, 1985; Muellerleile & Robertson, 2018). Much of the back-end technical infrastructure developments remained invisible to the masses and were not a discussion point in the civil or political realm, embodying the detachment of technological projects from social relations (León & Rosen, 2020)**.** Given that visibility is a vital condition for active reflection (Flyverbom, 2019; Greenwood & Cox, 2022), the opacity of such developments played a critical part in excluding public deliberations and shielding them from counter-hegemonic pressures.

4.6.3. State activity: Historical bloc's ideological indoctrination of the masses

Whereas the Estonian state retained a passive role in deferring the technological developments to tech experts, the historical bloc was more active in organizing a culture of technology towards the masses, which performed the role of ideological indoctrination towards the inevitability and utility of technology (Femia, 2011). In coercively promoting digital education to the populace through the Tiger Leap program, as well as the persuasive discourses around technology in the Estonian media, the historical bloc was able to diffuse the inevitability of digital technologies and moralize its uptake as the 'way forward' for the Estonian society. Additionally, the state along with economic actors also adopted persuasion tactics to facilitate citizens' familiarity with technologies through digital consumption, which serves to form consensus by showcasing the benefits of such technologies to the masses (Alvesson, 1985).

The neo-Gramscian approach highlights that a hegemonic social order complements coercion with developing consent structures in the cultural and social realm to legitimize its existence (Gill, 2008). In fact, civil society is a critical arena that constitutes the masses' common sense to stabilize and naturalize a social order, as well as produce counter-hegemonic struggles (Cox, 1999; Gramsci, 1971). The development of a robust and diverse civil society in Estonia was hindered due to the country's small size, culture of individualism, and a general consensus that the new state was not a foreign actor (D-Book). This allowed the state and economic actors to wield greater power in promoting their narratives in the civil realm and establish the value of the digital social order with greater effect. As a result, counter-hegemonic pressures were largely avoided, and the historical bloc – led by the state – was able to disseminate ideological indoctrination towards digitalization through coercive and persuasion tactics.

4.6.4. State re-engagement: Facilitating the universalization of digitalization

The technosolutionism efforts of tech experts had built the momentum to enable further technologization efforts. The hegemonic project of the e-ID card promoted the instrumental interests of the economic actors and reinforced consensus within the historical bloc by linking it to the state's desire for modernity (Levy & Egan, 2003; Maielli, 2015). The state relegated the development of the e-ID card to the economic actors due to the latter's technical expertise. Hence, the tech elite dominated the initiative and curtailed the involvement of the masses who were merely posited as potential beneficiaries (Beyes et al., 2022). Such a relationship between the state and the technological sector has previously been highlighted and even referred to as the internet-industrial complex (Flyverbom et al., 2019). However, in this instance, rather than utilizing the technologies already developed by the private sector, the state itself was persuaded by the narratives of techno-optimism to foster the very creation of the e-ID card through relegating its role. Nonetheless, as these developments were visible in the public realm, it invited contestations from political parties and the masses. Consequently, the state was persuaded by the economic actors to re-engage in its coercive capacities to make the e-ID card mandatory, which limited the masses' right to self-determination (Girei, 2016). Here, the state's re-engagement underscores its coercive power over its citizens while being a site of persuasion by the private tech sector.

Additionally, contestations – which were limited to the utility of the e-ID card – were pacified through persuading the masses by incrementally making private and public services accessible through it. Consequently, the state's dynamic roles of coercion – in mandating the card – and persuasion – through the induction of services – helped to universalize the applications of the e-ID card. This phase also highlights the role of the historical bloc in organizing the culture of technology in the civil realm to foster the masses' consensus and limiting their contestation to the utility of the e-ID card. Gramsci's idea of fostering consent of the masses relates to a psychological state involving some type of acceptance of the hegemonic order imposed by the historical bloc, rather than it being a reflection of their aspirations (Femia, 2011). As the masses, conditioned in the civil realm, lack the theoretical consciousness to completely comprehend their subaltern positions, their reduced contestation is effectively pacified by the historical bloc to retain the hegemonic social order (Femia, 2011). Through effective and enduring indoctrination of citizens' perspectives as well as the optimism surrounding internet technologies through state activity, the Estonian state indeed helped to shape the contestations against the digitalization drive. Furthermore, the historical bloc's persuasion tactics embody the principles of the technological ideology, which overcomes negation and contestation by promoting such developments as serving to benefit society, especially through a culture of benefit-inducing consumption to legitimize such development (Alvesson, 1985; Trittin-Ulbrich et al., 2021)**.** Gramsci (1971) also highlights that the interests of the subaltern group are partly considered to maintain the hegemony of dominant groups. Consequently, in being seduced through the benefits of convenience in online service delivery, citizens were naturalized in their subaltern role as consumers.

4.7. Concluding discussion

To conclude our chapter, we highlight the main contributions of our work. Our critical empirical contribution is to uncover the dynamic contestation and persuasion processes within a historical bloc which organized Estonia's post-Soviet digitalization drive, particularly focusing on the oft-ignored governing role of the state in both neo-Gramscian and digitalization scholarship. As previously discussed, while Gramsci himself considered the state to be an extremely important actor in enabling hegemony through its 'coercive armour' (1971), neo-Gramscian approaches in organization studies have "*overemphasized the power of private actors, such as corporations and NGOs*" (Bo et al., 2019, p. 1067) as governance in neoliberalism valorizes the ability of private actors to address societal and governance issues (Böhm et al., 2008; Girei, 2016; Levy & Egan, 2003; Levy & Scully, 2007). Scholarly efforts related to the governance of digital technologies espouse a similar tendency of state inaction as governments develop interdependencies with private actors due to the latter's expertise power for a variety of needs such as surveillance and developing technological solutions such as for smart cities (Alvesson, 1985; Flyverbom et al., 2019; León & Rosen, 2020; Whelan, 2019). Given the proliferation of digitalization in social, political, and economic life (Andriole, 2017; Leonardi & Treem, 2020; Parida et al., 2019; Vial, 2019), there are growing calls towards macro-level analyses that account for the role of the state and public policy in shaping digitalization initiatives (Bodrožić & Adler, 2022; Flyverbom et al., 2019). Towards this end, the case of Estonia's digitalization allows us to comprehensively investigate the governing role of the state vis-à-vis economic actors and civil society in orienting society towards digitalization.

Hence, our study also responds to calls for historicized and contextualized studies related to digital technologies (Beyes et al., 2022; Hensmans, 2021) by theorizing the 'socially contested' nature of the digitalization, which is formed through dynamic interactions between the state, economic actors, and civil society to govern a society towards digitalization. In doing so, we contribute towards scholarship by highlighting four modalities of the state's governing role in digitalization initiatives at a societal level in relation to tech experts and the economic actors: state idealization, state passivity, state activity, and state re-engagement. In state idealization, the Estonian state, in being seduced by the global structures of neoliberalism and modernity, valorized digital technologies which led to itself becoming an active site of persuasion by tech experts in the modality of state passivity. Simultaneously, the government also retained its governing ability through state activity towards the masses, referring to the employment of persuasive and coercive capacities to foster ideological indoctrination in the civil realm. Lastly, state re-engagement refers to the use of legislative powers and persuasion tactics to promote the interests of the historical bloc respectively.

Indeed, prior neo-Gramscian studies have dawn attention to the power dynamics within historical blocs, especially relating to private actors. Maieli (2015) has highlighted that the hegemonic projects, when in complementarity with structural hegemony, enable dominant actors to exert their influence within the hegemonic alliance. Through our theoretical model, we illustrate the ability of tech experts to 'link their agendas' (Girei, 2016, p. 206) to the state's desire for modernity through technosolutionism (Morozov, 2013)**.** This allows them to persuade the state to support continuous digitalization and even surrender its authority – through passivity and re-engagement – to govern the initiative.

We acknowledge that our qualitative analysis based on a single case-study limits the generalizability of our findings to other contexts and as a result, we encourage further investigations regarding the dynamic interactions in the state-business-civil society nexus to promote digitalization initiatives. For example, does the state maintain a passive role in the development of their technological infrastructure when foreign private-sector tech companies are involved? Also, whereas the Estonian digitalization was organic in that it was driven by the momentum built by the tech experts and the narratives of techno-optimism, how does the governing role of the state change when such initiatives are thoroughly planned and explicitly state-driven?

4.7.1. The shaping of civil society and contestations

This study also provides a unique perspective on the role of the civil society in the establishment of the digital hegemony. As the establishment of a social order requires both coercion and persuasion, civil society becomes "*the site through which ruling groups organize and construct consensus by diffusing and naturalizing certain values, worldviews and hierarchies*" (Morton, 2007, pp. 88–95). Our study, in analyzing the normalization of digitalization in the Estonian society, illustrates how the opaque nature of technological developments as well as the coercive and persuasion roles of the state shape civil society to limit contestation.

In examining the opaque and black box nature of technological development (Beyes et al., 2022; Pasquale, 2015), we assert that the historical bloc sustains its domination and averts counter-hegemonic pressures by depoliticizing infrastructural development through invisibilities. The opaque nature of technological developments relates to how disinterest is fostered in the masses and the civil realm, who perceive the developments to be marked by complexity (Muellerleile & Robertson, 2018). Given that visibility is an active condition for reflection (Flyverbom, 2019; Greenwood & Cox, 2022), technological developments escape the public eye for large periods of time and are sheltered from contestations. As Estonia's technological developments remained largely remained invisible or were dismissed as 'technical' matters in the civil realm, the masses were unable to avert them through counter-hegemonic pressures. Furthermore, in assessing the historical bloc's ideological indoctrination through organizing a culture of technology in Estonia, we showcase how the state adopts both persuasion and coercive measures to build consensus as well as shape contestations when technological developments became visible and are challenged. By mandating digital education and promoting digital consumption, the Estonian state adopted *coercive seduction* to foster digital inevitability within the masses and shape the contestation around the e-ID card to its utility, which was effectively managed by promoting more services.

Related to the neo-Gramscian approach, our study also contributes to prior literature by analyzing a context with a nascent civil society, which enabled the proliferation of a hegemonic digital regime. Most prior studies have analyzed the 'bottom-up contestations' from a developed civil society structure in relation to environmental governance (Levy et al., 2016). However, Estonia's digitalization efforts transpired upon its liberation from a Soviet-era rule, which was concurrent with the development of a budding civil society. Furthermore, the small population of the country and its individualistic culture, coupled with the nationalistic goal towards modernity, limited the diversity of the civil society and led to the historical bloc's efforts facing less contestations. Bo and colleagues (2019) have highlighted how the Chinese state faced bottom-up pressures from its nascent civil society, however these concerns were complemented by active awareness campaigns and monitoring by NGOs. In our case, as the internet technologies were at a nascent stage, the lack of debates in the global superstructures around privacy and surveillance facilitated the Estonian digital hegemony.

We posit that the effectiveness of Estonia's digital drive can be difficult to mirror in other contexts with a strong civil society in current times, when critiques of digital technologies and state distrust are rampant (Flyverbom et al., 2019; Zuboff, 2019). Consequently, we invite further research into this topic by exploring the social construction of other state-initiatives such as China's Social Credit System and India's Aadhaar program to investigate how global civil society actors and public awareness relating to state surveillance and privacy concerns shape the governance of digitalization initiatives.

4.8. References

Alaimo, C., & Kallinikos, J. (2016). Encoding the everyday: The infrastructural apparatus of social data. *Big Data Is Not a Monolith: Policies, Practices, and Problems*, 77–90.

Alvesson, M. (1985). A Critical Framework for Organizational Analysis. *Organization Studies*, *6*(2). https://doi.org/10.1177/017084068500600202

Andriole, S. J. (2017). SPRING 2017 ISSUE Five Myths About Digital Transformation. *MIT SLOAN MANAGEMENT REVIEW* , *58*(3).

Bates, T. R. (1975). Gramsci and the Theory of Hegemony. *Journal of the History of Ideas*, *36*(2). https://doi.org/10.2307/2708933

Bejerot, E., & Hasselbladh, H. (2013). Forms of Intervention in Public Sector Organizations: Generic Traits in Public Sector Reforms. *Organization Studies*, *34*(9), 1357–1380. https://doi.org/10.1177/0170840613477639

Beyes, T., Chun, W. H. K., Clarke, J., Flyverbom, M., & Holt, R. (2022). Ten Theses on Technology and Organization: Introduction to the Special Issue. *Organization Studies*, *43*(7), 1001–1018. https://doi.org/10.1177/01708406221100028

Bo, L., Böhm, S., & Reynolds, N. S. (2019). Organizing the Environmental Governance of the Rare-Earth Industry: China's passive revolution. *Organization Studies*, *40*(7). https://doi.org/10.1177/0170840618782278

Bodrožić, Z., & Adler, P. S. (2022). Alternative Futures for the Digital Transformation: A Macro-Level Schumpeterian Perspective. *Organization Science*, *33*(1). https://doi.org/10.1287/orsc.2021.1558

Böhm, S., Spicer, A., & Fleming, P. (2008). Infra-political dimensions of resistance to international business: A Neo-Gramscian approach. *Scandinavian Journal of Management*, *24*(3). https://doi.org/10.1016/j.scaman.2008.03.008

Bucher, E. L., Schou, P. K., & Waldkirch, M. (2021). Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy. *Organization*, *28*(1), 44–67.

Chenou, J. M., & Radu, R. (2019). The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business and Society*. https://doi.org/10.1177/0007650317717720

Cox, R. W. (1999). Civil society at the turn of the millenium: Prospects for an alternative world order. *Review of International Studies*, *25*(1). https://doi.org/10.1017/S0260210599000042

de Bakker, F., den Hond, F., King, B., & Weber, K. (2010). Special issue on "Social movements, civil societies and corporations." In *Organization Studies* (Vol. 31, Issue 7). https://doi.org/10.1177/0170840610376481

Eisenhardt, K. M. (1989). Eisenhardt 1989.pdf. *Academy of Management Review*.

Ellul, J. (1964). *The technological society*. Vintage.

Faraj, S., & Pachidi, S. (2021). Beyond Uberization: The co-constitution of technology and organizing. *Organization Theory*, *2*(1). https://doi.org/10.1177/2631787721995205

Femia, J. V. (2011). Gramsci's Political Thought. In *Gramsci's Political Thought*. https://doi.org/10.1093/acprof:oso/9780198275435.001.0001

Flyverbom, M. (2019). The digital prism transparency and managed visibilities in a datafied world. *The Digital Prism: Transparency and Managed Visibilities in a Datafied World*. https://doi.org/10.1017/9781316442692

Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business and Society*. https://doi.org/10.1177/0007650317727540

Fukuyama, F. (2006). *The end of history and the last man*. Simon and Schuster.

Gill, S. (2008). Power and resistance in the new world order: Second edition. In *Power and Resistance in the New World Order: Second Edition*. https://doi.org/10.1057/9780230584518

Girei, E. (2016). NGOs, Management and Development: Harnessing Counter-Hegemonic Possibilities. *Organization Studies*, *37*(2). https://doi.org/10.1177/0170840615604504

Gramsci, A. (1971). *Selections from the prison notebooks of Antonio Gramsci* (First Edition). International Publishers. https://search.library.wisc.edu/catalog/999473246802121

Greenwood, M., & Wolfram Cox, J. (2022). Seduced by Technology? How moral agency is mediated by the invisibility of everyday technologies. *Organization Studies*, 01708406221107455. https://doi.org/10.1177/01708406221107455

Han, B.-C. (2017). *Psychopolitics: Neoliberalism and New Technologies of Power*. Verso.

Hensmans, M. (2021). How digital fantasy work induces organizational ideal reversal? Long-term conditioning and enactment of digital transformation fantasies at a large alternative bank (1963–2019). *Organization*, *28*(1). https://doi.org/10.1177/1350508420968185

Jessop, B. (2010). Cultural political economy and critical policy studies. *Critical Policy Studies*, *3*(3–4). https://doi.org/10.1080/19460171003619741

Joseph, J. (2003). Hegemony: A realist analysis. In *Hegemony: A Realist Analysis*. https://doi.org/10.4324/9780203166529

Knudsen, J. S., & Moon, J. (2017). Visible Hands: Government Regulation and International Business Responsibility. In *Cambridge University Press*.

Kourula, A., Moon, J., Salles-Djelic, M. L., & Wickert, C. (2019). New Roles of Government in the Governance of Business Conduct: Implications for Management and Organizational Research. In *Organization Studies* (Vol. 40, Issue 8). https://doi.org/10.1177/0170840619852142

León, L. F. A., & Rosen, J. (2020). Technology as Ideology in Urban Governance. *Annals of the American Association of Geographers*, *110*(2). https://doi.org/10.1080/24694452.2019.1660139

Leonardi, P. M., & Treem, J. W. (2020). Behavioral Visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, *41*(12). https://doi.org/10.1177/0170840620970728

Levy, D. L., & Egan, D. (2003). A neo-Gramscian approach to corporate political strategy: Conflict and accommodation in the climate change negotiations. In *Journal of Management Studies* (Vol. 40, Issue 4). https://doi.org/10.1111/1467-6486.00361

Levy, D., Reinecke, J., & Manning, S. (2016). The Political Dynamics of Sustainable Coffee: Contested Value Regimes and the Transformation of Sustainability. *Journal of Management Studies*, *53*(3). https://doi.org/10.1111/joms.12144

Levy, D., & Scully, M. (2007). The institutional entrepreneur as modern prince: The strategic face of power in contested fields. *Organization Studies*, *28*(7). https://doi.org/10.1177/0170840607078109

Maielli, G. (2015). Explaining Organizational Paths through the Concept of Hegemony: Evidence from the Italian Car Industry. In *Organization Studies* (Vol. 36, Issue 4). https://doi.org/10.1177/0170840614561565

Marcuse, H. (2013). *One-dimensional man: Studies in the ideology of advanced industrial society*. Routledge.

Marquis, C., & Qiao, K. (2020). Waking from Mao's Dream: Communist Ideological Imprinting and the Internationalization of Entrepreneurial Ventures in China. *Administrative Science Quarterly*, *65*(3). https://doi.org/10.1177/0001839218792837

Mees-Buss, J., & Welch, C. (2019). Managerial Ideologies Dividing the Corporate Elite: A process study of the rise and fall of a counter-ideology. *Organization Studies*, *40*(4). https://doi.org/10.1177/0170840617747920

Moog, S., Spicer, A., & Böhm, S. (2015). The Politics of Multi-Stakeholder Initiatives: The Crisis of the Forest Stewardship Council. *Journal of Business Ethics*, *128*(3). https://doi.org/10.1007/s10551-013-2033-3

Morozov, E. (2013). To save everything, click here : the folly of technological solutionism / Evgeny Morozov. *To Save Everything, Click Here : The Folly of Technological Solutionism*.

Morton, A. D. (2007). Waiting for Gramsci: State formation, passive revolution and the international. *Millennium: Journal of International Studies*, *35*(3). https://doi.org/10.1177/03058298070350031301

Muellerleile, C., & Robertson, S. L. (2018). Digital Weberianism: Bureaucracy, Information, and the Techno-rationality of Neoliberal Capitalism. *Indiana Journal of Global Legal Studies*, *25*(1). https://doi.org/10.2979/indjglolegstu.25.1.0187

Parida, V., Sjödin, D., & Reim, W. (2019). Reviewing literature on digitalization, business model innovation, and sustainable industry: Past achievements and future promises. In *Sustainability (Switzerland)* (Vol. 11, Issue 2). https://doi.org/10.3390/su11020391

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

Peticca-Harris, A., DeGAMA, N., & Ravishankar, M. N. (2020). Postcapitalist precarious work and those in the 'drivers' seat: Exploring the motivations and lived experiences of Uber drivers in Canada. *Organization*, *27*(1), 36–59.

Reinecke, J., Van Bommel, K., & Spicer, A. (2017). When orders of worth clash: Negotiating legitimacy in situations of moral multiplexity. *Research in the Sociology of Organizations*. https://doi.org/10.1108/S0733-558X20170000052002

Seeck, H., Sturdy, A., Boncori, A. L., & Fougère, M. (2020). Ideology in Management Studies. *International Journal of Management Reviews*, *22*(1). https://doi.org/10.1111/ijmr.12215

Strauss, A., & Corbin, J. (1990). Basics of Qualitative Research: Grounded Theory Procedures and Techniques. In *Handbook of qualitative research*.

Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, *28*(1), 8–25.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/J.JSIS.2019.01.003

Whelan, G. (2019). Born Political: A Dispositive Analysis of Google and Copyright. *Business and Society*. https://doi.org/10.1177/0007650317717701

Wittneben, B. B. F., Okereke, C., Banerjee, S. B., & Levy, D. L. (2012). Climate Change and the Emergence of New Organizational Landscapes. *Organization Studies*, *33*(11). https://doi.org/10.1177/0170840612464612

Zuboff, S. (2015). Big Other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*, 75–89.

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs.

Chapter 5. General Conclusion

The overarching research question of this thesis relates to: how are relations of power and resistance organized between business, state, and citizens in relation to digitalization? Digitalization has been explored in academic literature in terms of the affordances it enables towards addressing organizational and societal problems (Majchrzak et al., 2016; McAfee & Brynjolfsson, 2012; Vial, 2019; von Krogh, 2018), as well as the various controversies associated with its solutionist ideology that can reproduce inequalities and avert its democratic potential (Martin, 2016a; Trittin-Ulbrich et al., 2021; Zuboff, 2019)**.** There have also been growing calls to address the role of the state and civil society actors in addressing the negative consequences of unfettered digitalization (Bodrožić & Adler, 2022; Finck, 2018; Knudsen & Moon, 2017). While these issues indeed are critical to be addressed by organizational studies scholarship, surprisingly, the underlying datafication processes as well as issues of systemic power have generally been taken-for-granted. For example, in highlighting the effects of workplace surveillance and precarity of gig economy workers (Bucher et al., 2021; Peticca-Harris et al., 2020; Walker et al., 2021), digitalization has merely been posited as the new face, or even continuation, of capitalism while the underlying datafication practices have not been analyzed enough.

It is towards such a gap that this thesis aims to bring in the constructs of power as captured by hegemony, privacy, and resistance to discuss how relations between the state, businesses and citizens are organized, in a bid to understand the socially contested nature of digitalization (Beyes et al., 2022). In undertaking a meso-macro lens through the three main chapters of the thesis, a deeper understanding of these relations is possible in the context of digitalization and its related datafication processes.

By exploring resistance and state action against the datafication practices of major platforms and corporations, this thesis enables a better comprehension of the effectiveness of such efforts against the growing platform power. Additionally, in highlighting the role of the state and tech elites towards establishing digitalization initiatives, this thesis uncovers the dynamic interactions between state-business nexus (Flyverbom, 2019) based on mutually shared interests through a historical analysis. Insights from this thesis reveals the multi-layered relationship between the state and corporations relating to digitalization, wherein the state must balance the promotion of such technologies with curbing the potential harms associated with their underlying datafication efforts. Taken together, in assessing the power relations involved in digitalization, this thesis seeks to reveal the roles of varied actors to generate socially responsible digitalization.

5.1. Theoretical contributions

Specifically, this thesis highlights resistance, hitherto mainly glossed over in the lived experiences of gig economy workers, as a critical avenue for addressing challenges and contestations towards the regimes of datafication. The second chapter of this thesis, in corresponding to the contextual nature of resistance (Mumby et al., 2017), undertakes this task to enrich organizational studies by exploring how datafication of private corporations are challenged by data activist entities. While resistance literature is critiqued for promoting banal acts that do not adequately challenge the dominant regimes (Fleming, 2016), this chapter contributes to the literature stream by explicitly delineating acts of complicity with and confrontation against the dispossessive datafication practices of corporations. I acknowledge the ideological work of corporations – a form of systemic power – which naturalize datafication practices to present how resistance occurs in a convoluted setting of smart power (Han, 2017), whereby exploitation is less perceptible due to it valorizing personal freedom and benefits. In charting the data flows associated with the resistance strategies proposed by these entities, I propose a theoretical typology of the 'Janus face of resistance', wherein the confrontation and complicity of resistance are simultaneously exposed in the digital realm. Indeed, resistance against datafication is often dependent on the very data that is the source of exploitation, especially in relation to enabling citizens to utilize it towards garnering additional benefits. However, given the informational asymmetries and naturalization of data extractivism practices that mark the digital realm, the exploitative datafication processes can assume the role of the 'object of resistance' (Taskin et al., 2022), enabling greater visibility into how invisible regimes exert their power. Such practices can lead to greater politicization of the naturalized datafication practices while other strategies – such as the separation of service delivery from data capture – can pave the way for alternative business models (Zanoni et al., 2017),. Given the complex nature of datafication practices, such nuanced understandings of resistance enrich scholarship by accounting for the specificities of the digital context.

This thesis also contributes to the oft-ignored role of the state and political institutions in relation to digitalization (Bodrožić & Adler, 2022; Flyverbom et al., 2019). Particularly relating to datafication, Chapter 3 of this thesis sheds light on how regulatory efforts – EU's GDPR – can reassert and diminish citizens' right to privacy, in a bid to address the power imbalances that are tilted in favour of digital platforms. Such a study also highlights the shift away from self-regulation of corporations towards the reengagement of the state (Cammaerts & Mansell, 2020; Finck, 2018; Knudsen & Moon, 2017). Whereas chapter 2 problematizes the dispossessive data production processes as a source of exploitation, Chapter 3 contributes to the scholarly literature by analyzing how state action seeks to empower citizens both in relation to such production processes, as well as post-datafication practices of private corporations. Hence, while narratives of privacy being dead are prevalent, it is important to note that such a concept is indeed an aspect of power, as it challenges the dominant system of datafication in play. In doing so, we propose that a normative, dynamic approach to privacy – captured by the social contracts view (Martin, 2016b) – offers an empowering avenue to protect citizens, wherein they maintain expectations over the collection and utilization of their data. Relating to the literature on the social contracts theory (Donaldson & Dunfee, 1999), this study contributes by overcoming the criticism on the lack of application of this theory to express how it can be used to assess the efficacy of regulatory action against normative expectations.

Furthermore, the continued involvement of citizens in relation to the production and control of their data presents a double-edged sword. On one hand, it reasserts their ownership of the data that is produced about them, empowering them to continuously assert their expectations over how data assets are utilized. However, on the other hand, in doing so, such practices contribute to self-management of data by these very citizens, which can be overbearing and lead to digital resignation (Draper & Turow, 2019). Herein, this study also contributes to a better conceptualization of the practical implications associated with the privacy paradox (Martin, 2020), wherein citizens express desire for privacy but are often seen to willingly share whatever data is sought from them. We highlight citizens may not only *willingly* share their data but can rather be overcome with additional responsibilities through the self-management of their data, for which they are neither competent nor completely aware. Hence, state action to protect citizens from datafication practices can, indeed, both empower and disempower citizens in relation to platform power.

In addition to indicating the reengagement of political institutions to protect citizens' interests, this thesis also uncovers the state-business-civil society nexus through which digitalization unfolds in society, rendering citizens as mere consenting audiences to such development. Chapter 4 contributes to organization studies' scholarship by delineating the governing role of the state in digitalization efforts, which has often been overlooked in favour of private actors (Bowie & Jamal, 2006; Faraj & Pachidi, 2021). In bringing the concept of hegemony to digitalization studies (Gramsci, 1971; Levy & Egan, 2003), we show how systemic power – reflected in the ideology of digitalization – is organized by the state and private actors to be accepted by society and how it can be situated historically and geographically. This study also contributes to the calls that highlight the study of digitalization at a macro level (Bodrožić & Adler, 2022). In delineating the solutionism and optimism involved with digital technologies (Alvesson, 1985; León & Rosen, 2020; Morozov, 2013; Muellerleile & Robertson, 2018), this chapter provides historical evidence to theorize four modalities of the governing role of the state: *state idealization, state passivity, state activity* and *state re-engagement.* Taken together, these indicate how the state surrenders control of technological developments, while continuously facilitating them, to the tech elite. Simultaneously, the state along with the private actors coerce and persuade citizens to generate consent towards such developments. While previous studies have highlighted the dependency of the state on the tech elite, this study uncovers the dynamic interactions between such a 'historical bloc' (Gramsci, 1971) – showing the state to be both a site of persuasion by the tech elite and a conduit for persuasion and coercion towards the masses – to delineate how the naturalization of digitalization occurs at a societal scale. Relatedly, we link the invisible nature of technological developments, as well as their ability to foster disinterest of the masses through complexity (Flyverbom, 2019; Muellerleile & Robertson, 2018), as a critical factor in limiting contestations against such developments. Hence, the democratic potential of digital technologies can be problematized as their own development, while political in its very nature (Whelan, 2019), can be seen as excluding contestation and involvement of the masses.

5.2. Practical implications

Given that the need for organization studies' scholarship to generate practical impact has been widely discussed (Simsek et al., 2022; Zahra & Newey, 2009), it is critical that this thesis generates valuable insights for non-academic actors. There are three non-academic audiences that can avail the insights from this thesis to enable responsible and inclusive digitalization initiatives: business entities including alternative organizations, policymakers, and civil society actors.

Numerous studies have illustrated the harmful impacts of digitalization due to the data practices and instrumental interests of private corporations (Martin, 2016a, 2018; Trittin-Ulbrich et al., 2021). One of the critical elements that needs addressing is how data has gone from becoming a part of the business to becoming business itself, captured in quips such as 'data is the new oil' (The Economist, 2017). With growing social backlash against such practices which can challenge the legitimacy of private corporations, findings from the second and third chapter of this thesis can serve to inform business managers about fostering responsible data practices. While we problematize and capture the resistance against accumulation by dispossession datafication practices of corporations, these chapters reveal that data minimization – which refers to the need to only collect that data which is absolutely necessary for service provisioning – is a principle that can reduce unethical data collection and protect corporations from social backlash. While it is true that major digital corporations such as Meta and Alphabet have increasingly become more powerful despite unethical practices in the digital realm, we propose that conducting business operations with a normative principle of data minimization can indeed safeguard emerging and established organizations from the growing social backlash.

Furthermore, a normative and dynamic understanding of privacy as a social contract – as presented in Chapter 3 – can enable greater sensitivity in the collection and utilization of users' data, enabling business managers to foster responsible digital solutions. Having a dynamic view of their users' privacy expectations can not only inform the ethical choices that business managers and chief data officers make with such data, but it can also encourage greater investments in data security to prevent post-datafication privacy-violating breaches. Additionally, it is important to highlight that the action of separating data collection from service delivery – as proposed by some data activist entities in Chapter 2 – presents a promising avenue for alternative organizing. This idea has gained some traction due to the narratives of influential figures such as Tim Berners-Lee, the founder of the internet. In doing so, data can remain a part of business, rather than becoming the business itself**.**

In addition to business managers and alternative organizers, this thesis serves to inform policymakers in political institutions. Digitalization, especially when coupled with the dominant neoliberal ideology, initially limited the role of the state while valorizing ideals of self-regulation (Berg, 2019). However, the sustained unethical practices of digital platforms have led to calls for the reengagement of the state (Cammaerts & Mansell, 2020; Chenou & Radu, 2019; Finck, 2018; Knudsen & Moon, 2017). Chapter 3 of this thesis illustrates such a reengagement, explicating how the provision of data rights to empower its citizens against the datafication practices of private corporations can enable their greater involvement in relation to their personal data. Our findings indicating how citizens are overburdened in self-managing their privacy due to their cognitive and temporal limitations serve as a critical insight towards the growing questions surrounding the efficacy of the GDPR in practice (Andrew & Baker, 2021; Schade, 2023). Indeed, consenting to data collection may not be an active choice but rather a function of information overload and digital resignation. Hence, it can be proposed that state regulations to curb platform power, especially in relation to datafication, must pay greater attention to accountability measures rather than merely mandating the provision of citizens' consent. In this regard, data protection inspectorates of countries need to be empowered as a state enforcement measure to proactively monitor and control the unethical data practices of private corporations that foster coercive consent. Doing so can more adequately reinforce the state's role of protecting its citizens from the harmful effects of digitalization.

With the ubiquity of digitalization, civil society organizations are indeed becoming important players to voice concern over its negative implications for citizens and society (Beraldo & Milan, 2019; Lehtiniemi & Ruckenstein, 2019). It is indeed true that digitalization initiatives have often excluded the role of societal actors by fostering disinterest in the masses, who view such developments as marred with extreme technical complexity (León & Rosen, 2020; Muellerleile & Robertson, 2018). In recent years, we are seeing news (Cadwalladr & Graham-Harrison, 2018) and entertainment media – television shows such as *The Black Mirror* and documentaries such as *The Social Dilemma* – undertaking a greater role in shedding light on the harmful effects of digital technologies and datafication processes. Social movements have often focused heavily on the instrumentalization of personal data by private actors at the expense of the data-producing citizens while promulgating the need to create mutually beneficial outcomes (Beraldo & Milan, 2019; Lehtiniemi & Ruckenstein, 2019). As we highlight, the ideological work of smart power underlies the datafication processes of private corporations and reduces the perceptibility of such exploitation. This thesis presents practical implications for civil society actors to counter platform power by politicizing the ideological work that enables extensive data capture, such as by the resistance through denaturalizing datafication strategy as seen in Chapter 2. In doing so, greater pressure at the grassroots level can be created and placed on the political elite to make the surveillance-based data extraction processes an important agenda in political discussions and actions, while expanding debates beyond their mere social utility of digitalization.

Furthermore, Chapter 4 of this thesis highlights how civil society itself is shaped and influenced by the state-business nexus to promote digitalization. The digitalization of governmental infrastructure has also become commonplace for purposes such as delivering public services and enabling efficiency (Bloomfield & Hayes, 2009). With the state itself becoming a site of persuasion by the technological elite, especially through espousing the logics of "technique" (Ellul, 1964), such developments are sheltered from contestation due to their invisibility in the civil realm. In this regard, social movements and civil society actors must pay close attention to public-sector digitalization initiatives in order to create visibility and awareness at a societal level. Greater efforts must also be undertaken to involve the diversity of expert and citizen perspectives in such developments. Such diversity of views in civil society regarding digitalization, which was not visible in Estonia's digitalization drive as seen in Chapter 4, can overcome the persuasive tactics of the state-business nexus and lead to more balanced and inclusive digital developments.

5.3. Limitations and future research

As with any academic research, this thesis contains certain limitations. In regards to the methodology, the second chapter of this thesis conducts a qualitative content analysis of the narratives and offerings of self-proclaiming data activists. Such a methodology only presents a snap-shot view of the resistance strategies proposed by these entities, which limits the development of robust insights into how they interact with an array of societal actors to accomplish their stated missions. Additionally, it limits the understanding of if and how these entities, when facing market pressure, experience alterations in their mission, leading them towards greater complicity with the dominant regimes of datafication (Dahlman et al., 2022; Ometto et al., 2019). Is it possible that a change in the organizational make-up of these entities, ranging from employees' turnover to a change in leadership, contributes to potential mission drifts – both in terms of confrontational resistance becoming more complicit and complicit resistance becoming more confrontational? While we sacrificed depth for breadth in compiling the resistance strategies in this study, longitudinal case-studies can certainly serve as fruitful avenues to explore these questions and expand scholarship on the evolving nature of resistance in the digital realm. Additionally, the sample compiled for this study is not comprehensive. For example, public data centers and data funds (Micheli et al., 2020) were not considered in this study. Future research can, indeed, enrich the scholarship at the intersection of critical data studies and organization studies to highlight the power relations that govern them, as well as their potentiality in enabling sustainable digital futures.

While the third chapter of this doctoral thesis presents an analysis of the EU's GDPR, which has been categorized as the 'gold standard' (Andrew & Baker, 2021) of data protection regulations, our analysis focuses primarily on the provision of data rights and accountability measures through which citizens' privacy is protected. However, the strong interplay between the state-business nexus is an important factor in the shaping of regulations, which often leads to the promotion of corporations' interests (Chenou & Radu, 2019; Trittin-Ulbrich et al., 2021; Whelan, 2019). In this regard, we have not shed light on the processes and negotiations between corporations and the state through which the specificities of this regulation were finalized. How was the formulation of the GDPR informed by corporations? Which of their interests were accommodated and contested by the state? What types of narratives did these corporations employ in promoting their interests, while reducing the regulatory oversight mechanisms proposed by the state actors? Utilizing literature on corporate political activity (Chenou & Radu, 2019; Whelan, 2019), these questions can reveal more about platforms' power as well as their strategies to persuade the state towards business-friendly regulations.

Another limitation of this thesis relates to its rather Eurocentric focus. In addition to the fact that over 70% of the sample in chapter 2 was comprised of European-based data activists, the third and fourth chapter of the thesis, focusing on the EU's GDPR and Estonia's digitalization drive, are also situated within the European context. Digitalization, characterized by its ubiquity, indeed impacts countries around the world. For example, 137 countries have adopted some form of data protection regulation, which offers a critical avenue to explore the role of the state in protecting their citizens' privacy vis-à-vis private corporations' datafication practices (United Nations Conference on Trade and Development, 2023). Then, we highlight that while we have presented a normative definition of privacy as a social contract, it is critical to note that privacy is contextual (Nissenbaum, 2004). Herein, organization and business ethics scholarship can be enriched in uncovering how privacy in the digital realm is understood in non-Western setting, such as those marked by collective cultures? Is the surrendering of expectations over the use of data more common in those settings with extreme patriotism, or where the state is considered to be a nurturer? What types of systemic power is more commonly employed in naturalizing digitalization in society in non-Western settings?

Furthermore, while we acknowledge the presence of major Chinese platforms, the most commonly used digital platforms around us are generally Western in their origin. This presents a novel angle in uncovering insights relating to data and digital colonialism (Couldry & Mejias, 2019). How does the data-dependent relationship change between the state and digital platforms, when the latter is a foreign entity? Indeed, we have seen major corporations like Facebook publicly challenge requests from the Chinese government, while simultaneously acquiescing to them by setting up subsidiaries in those countries with less regulatory oversight. Hence, a geopolitical lens on the state-business nexus can also contribute to scholarship relating to power relations and governance in the age of digitalization.

We also acknowledge that the dynamic and diverse role of the global civil society (Frangonikolopoulos, 2012) is not thoroughly captured in this thesis as much as it deserves to be given the interconnected and globalized nature of the world, and especially in the digital realm. Rather, we have focused on those actors which are situated within particular political entities – such as the EU – or a specific nation-state, as in the case of Estonia in the fourth chapter. The hegemony of digitalization that was established in Estonia was assisted by the fact that at such a time, the narratives around the internet were brimming with optimism while issues of privacy were not salient. However, as times have changed, these issues indeed have become more pervasive in society and are often presented by actors of the global civil society – such as foreign press, international organizations, and think tanks. Future studies, in utilizing social movements and community literature, can certainly investigate how local civil society actors and citizens respond to and/or acknowledge those concerns related to digitalization which are propagated by global actors. How are contestations promulgated by global civil society actors against controversial state-directed digitalization initiatives received by the local citizens? For example, how do Chinese citizens respond to foreign criticisms regarding the Chinese Social Credit system? Such studies can also leverage a geopolitical lens to uncover such power relations.

Given the specific focus on this doctoral thesis and its specific chapters, indeed, the avenues for future research that I posit are not exhaustive. However, they certainly can enrich the emerging scholarship on the dark side of digitalization (Trittin-Ulbrich et al., 2021; Zuboff, 2019) as well as the relations of power and resistance through exploring the nuances of the digital realm. To conclude, the impact of digitalization on organizations and society cannot be underestimated. In addition to its ability to enable promising avenues of democratization and participation, its ability to shape power relations between the nexus of state-business-citizens becomes fundamentally more important. In acknowledging its ubiquity, organizational scholarship must remain attuned to the systemic power underlying digitalization and contestations against it in order to responsibly direct such technologies to create a fairer, more sustainable world.

5.4. References

Ahmadi, M., Dileepan, P., & Wheatley, K. K. (2016). A SWOT analysis of big data. *Journal of Education for Business*, *91*(5), 289–294. https://doi.org/10.1080/08832323.2016.1181045

Alaimo, C. (2022). From People to Objects: The digital transformation of fields. *Organization Studies*, *43*(7). https://doi.org/10.1177/01708406211030654

Albu, O. B., & Flyverbom, M. (2019). Organizational Transparency: Conceptualizations, Conditions, and Consequences. *Business and Society*. https://doi.org/10.1177/0007650316659851

Alghamdi, N. S., & Alghamdi, S. M. (2022). The Role of Digital Technology in Curbing COVID-19. In *International Journal of Environmental Research and Public Health* (Vol. 19, Issue 14). https://doi.org/10.3390/ijerph19148287

Alvesson, M. (1985). A Critical Framework for Organizational Analysis. *Organization Studies*, *6*(2). https://doi.org/10.1177/017084068500600202

Andrew, J., & Baker, M. (2021). The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business Ethics*, *168*(3). https://doi.org/10.1007/s10551-019-04239-z

Andriole, S. J. (2017). SPRING 2017 ISSUE Five Myths About Digital Transformation. *MIT SLOAN MANAGEMENT REVIEW* , *58*(3).

Baikovich, A., Wasserman, V., & Pfefferman, T. (2021). 'Evolution from the inside out': Revisiting the impact of (re) productive resistance among ultra-orthodox female entrepreneurs. *Organization Studies*, 01708406211024574.

Benner, M. J., & Waldfogel, J. (2023). Changing the channel: Digitization and the rise of "middle tail" strategies. *Strategic Management Journal*, *44*(1). https://doi.org/10.1002/smj.3130

Beraldo, D., & Milan, S. (2019). From data politics to the contentious politics of data. *Big Data and Society*. https://doi.org/10.1177/2053951719885967

Berg, C. (2019). Regulate?: Innovate! *Institute of Public Affairs Review: A Quarterly Review of Politics and Public Affairs, The*, *71*(2), 32.

Beverungen, A., Beyes, T., & Conrad, L. (2019). The organizational powers of (digital) media. *Organization*, *26*(5), 621–635.

Beyes, T., Chun, W. H. K., Clarke, J., Flyverbom, M., & Holt, R. (2022). Ten Theses on Technology and Organization: Introduction to the Special Issue. *Organization Studies*, *43*(7), 1001–1018. https://doi.org/10.1177/01708406221100028

Birks, J. (2014). Networks of Outrage and Hope: Social Movements in the Internet Age. *European Journal of Communication*, *29*(5). https://doi.org/10.1177/0267323114539430c

Bloomfield, B. P., & Hayes, N. (2009). Power and organizational transformation through technology: Hybrids of electronic government. *Organization Studies*, *30*(5). https://doi.org/10.1177/0170840609104394

Bodrožić, Z., & Adler, P. S. (2022). Alternative Futures for the Digital Transformation: A Macro-Level Schumpeterian Perspective. *Organization Science*, *33*(1). https://doi.org/10.1287/orsc.2021.1558

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the Internet: Self-regulation or government regulation? *Business Ethics Quarterly*. https://doi.org/10.5840/beq200616340

Bucher, E. L., Schou, P. K., & Waldkirch, M. (2021). Pacifying the algorithm–Anticipatory compliance in the face of algorithmic management in the gig economy. *Organization*, *28*(1), 44–67.

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*.

Cammaerts, B., & Mansell, R. (2020). Digital Platform Policy and Regulation: Toward a Radical Democratic Turn. *International Journal of Communication*.

Castelló, I., Etter, M., & Årup Nielsen, F. (2016). Strategies of Legitimacy Through Social Media: The Networked Strategy. *Journal of Management Studies*, *53*(3). https://doi.org/10.1111/joms.12145

Castelló, I., Morsing, M., & Schultz, F. (2013). Communicative Dynamics and the Polyphony of Corporate Social Responsibility in the Network Society. In *Journal of Business Ethics* (Vol. 118, Issue 4). https://doi.org/10.1007/s10551-013-1954-1

Castells, M. (2017). 75. Networks of Outrage and Hope: Social Movements in the Internet Age. In *Democracy*. https://doi.org/10.7312/blau17412-091

Chen, Y. H., & Barnes, S. (2007). Initial trust and online buyer behaviour. *Industrial Management and Data Systems*. https://doi.org/10.1108/02635570710719034

Chenou, J. M., & Radu, R. (2019). The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business and Society*. https://doi.org/10.1177/0007650317717720

Cho, D., Smith, M. D., & Zentner, A. (2016). Internet adoption and the survival of print newspapers: A country-level examination. *Information Economics and Policy*, *37*. https://doi.org/10.1016/j.infoecopol.2016.10.001

Christl, W., & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. https://crackedlabs.org/en/networksofcontrol

Clarke, R. (2003). Dataveillance – 15 Years On. *Privacy Issues Forum*.

Collier, M. (2020). Review: Capital Is Dead: Is This Something Worse? , by McKenzie Wark . *Afterimage*, *47*(1). https://doi.org/10.1525/aft.2020.471016

Contu, A. (2008). Decaf Resistance: On Misbehavior, Cynicism, and Desire in Liberal Workplaces. *Management Communication Quarterly*, *21*(3), 364–379. https://doi.org/10.1177/0893318907310941

Correani, A., De Massis, A., Frattini, F., Petruzzelli, A. M., & Natalicchio, A. (2020). Implementing a Digital Strategy: Learning from the Experience of Three Digital Transformation Projects. *California Management Review*, *62*(4). https://doi.org/10.1177/0008125620934864

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media*, *20*(4), 336–349.

Couldry, N., & Yu, J. (2018). Deconstructing datafication's brave new world. *New Media and Society*. https://doi.org/10.1177/1461444818775968

Courpasson, D. (2017). Beyond the Hidden/Public Resistance Divide: How Bloggers Defeated a Big Company. *Organization Studies*, *38*(9), 1277–1302. https://doi.org/10.1177/0170840616685363

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues*. https://doi.org/10.1111/1540-4560.00067

Dahlman, S., Mygind du Plessis, E., Husted, E., & Just, S. N. (2022). Alternativity as freedom: Exploring tactics of emergence in alternative forms of organizing. *Human Relations*, *75*(10). https://doi.org/10.1177/00187267221080124

Donaldson, T., & Dunfee, T. W. (1999). Ties That Bind: A Social Contracts Approach to Business Ethics. In *Academy of Management Perspectives* (Vol. 13, Issue 4). https://doi.org/0875847277

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media and Society*. https://doi.org/10.1177/1461444819833331

Ellul, J. (1964). *The technological society*. Vintage.

Elmholdt, K. T., Elmholdt, C., & Haahr, L. (2021). Counting sleep: Ambiguity, aspirational control and the politics of digital self-tracking at work. *Organization*, *28*(1). https://doi.org/10.1177/1350508420970475

Etter, M., & Albu, O. B. (2021). Activists in the dark: Social media algorithms and collective action in two social movement organizations. *Organization*, *28*(1), 68–91.

Etter, M., Fieseler, C., & Whelan, G. (2019). Sharing Economy, Sharing Responsibility? Corporate Social Responsibility in the Digital Age. *Journal of Business Ethics*, *159*(4). https://doi.org/10.1007/s10551-019-04212-w

Faraj, S., & Pachidi, S. (2021). Beyond Uberization: The co-constitution of technology and organizing. *Organization Theory*, *2*(1). https://doi.org/10.1177/2631787721995205

Finck, M. (2018). Digital co-regulation: Designing a supranational legal framework for the platform economy. *European Law Review*. https://doi.org/10.2139/ssrn.2990043

Fleming, P. (2016). Resistance and the "post-recognition" turn in organizations. *Journal of Management Inquiry*, *25*(1), 106–110.

Fleming, P., & Spicer, A. (2003). Working at a cynical distance: Implications for power, subjectivity and resistance. *Organization*, *10*(1), 157–179.

Fleming, P., & Spicer, A. (2008). Beyond power and resistance: New approaches to organizational politics. *Management Communication Quarterly*, *21*(3), 301–309.

Fleming, P., & Spicer, A. (2014). Power in Management and Organization Science. *Academy of Management Annals*, *8*(1). https://doi.org/10.1080/19416520.2014.875671

Flick, U., & Schreier, M. (2014). Qualitative Content Analysis. In *The SAGE Handbook of Qualitative Data Analysis*. https://doi.org/10.4135/9781446282243.n12

Flyverbom, M. (2019). The digital prism transparency and managed visibilities in a datafied world. *The Digital Prism: Transparency and Managed Visibilities in a Datafied World*. https://doi.org/10.1017/9781316442692

Flyverbom, M., Deibert, R., & Matten, D. (2019). The Governance of Digital Technology, Big Data, and the Internet: New Roles and Responsibilities for Business. *Business and Society*. https://doi.org/10.1177/0007650317727540

Foucault, M. (1978). The history of sexuality (R. Hurley, Trans.). *New York: Pantheon*.

Frangonikolopoulos, C. A. (2012). Global civil society and deliberation in the digital age. *International Journal of Electronic Governance*, *5*(1). https://doi.org/10.1504/IJEG.2012.047440

Gill, S. (2008). Power and resistance in the new world order: Second edition. In *Power and Resistance in the New World Order: Second Edition*. https://doi.org/10.1057/9780230584518

Gramsci, A. (1971). *Selections from the prison notebooks of Antonio Gramsci* (First Edition). International Publishers. https://search.library.wisc.edu/catalog/999473246802121

Greenwood, M., & Wolfram Cox, J. (2022). Seduced by Technology? How moral agency is mediated by the invisibility of everyday technologies. *Organization Studies*, 01708406221107455. https://doi.org/10.1177/01708406221107455

Han, B.-C. (2017). *Psychopolitics: Neoliberalism and New Technologies of Power*. Verso.

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A Systematic Review of the Literature on Digital Transformation: Insights and Implications for Strategy and Organizational Change. *Journal of Management Studies*, *58*(5). https://doi.org/10.1111/joms.12639

Hensmans, M. (2021). How digital fantasy work induces organizational ideal reversal? Long-term conditioning and enactment of digital transformation fantasies at a large alternative bank (1963–2019). *Organization*, *28*(1). https://doi.org/10.1177/1350508420968185

Jamil, S. (2022). Postulating the Post-Arab Spring Dynamics of Social Media & Digital Journalism in the Middle East. *Digital Journalism*, *10*(7). https://doi.org/10.1080/21670811.2022.2040040

Jesse, M., & Jannach, D. (2021). Digital nudging with recommender systems: Survey and future directions. In *Computers in Human Behavior Reports* (Vol. 3). https://doi.org/10.1016/j.chbr.2020.100052

Karatzogianni, A., & Robinson, A. (2014). Digital prometheus: Wikileaks, the state-network dichotomy, and the antinomies of academic reason. *International Journal of Communication*, *8*(1).

Kassner, L., Hirmer, P., Wieland, M., Steimle, F., Königsberger, J., & Mitschang, B. (2017). The social factory: Connecting people, machines and data in manufacturing for context-aware exception escalation. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2017-January*. https://doi.org/10.24251/hicss.2017.202

Knudsen, J. S., & Moon, J. (2017). Visible Hands: Government Regulation and International Business Responsibility. In *Cambridge University Press*.

Kuusisto, M. (2017). Organizational effects of digitalization: A literature review. In *International Journal of Organization Theory and Behavior* (Vol. 20, Issue 3). https://doi.org/10.1108/ijotb-20-03-2017-b003

Kwon, W., & Constantinides, P. (2018). Ideology and Moral Reasoning: How wine was saved from the 19th century phylloxera epidemic. *Organization Studies*, *39*(8). https://doi.org/10.1177/0170840617708006

Labrecque, L. I., vor dem Esche, J., Mathwick, C., Novak, T. P., & Hofacker, C. F. (2013). Consumer power: Evolution in the digital age. *Journal of Interactive Marketing*. https://doi.org/10.1016/j.intmar.2013.09.002

Lehtiniemi, T., & Ruckenstein, M. (2019). The social imaginaries of data activism. *Big Data and Society*. https://doi.org/10.1177/2053951718821146

León, L. F. A., & Rosen, J. (2020). Technology as Ideology in Urban Governance. *Annals of the American Association of Geographers*, *110*(2). https://doi.org/10.1080/24694452.2019.1660139

Leonardi, P. M., & Treem, J. W. (2020). Behavioral Visibility: A new paradigm for organization studies in the age of digitization, digitalization, and datafication. *Organization Studies*, *41*(12). https://doi.org/10.1177/0170840620970728

Levy, D. L., & Egan, D. (2003). A neo-Gramscian approach to corporate political strategy: Conflict and accommodation in the climate change negotiations. In *Journal of Management Studies* (Vol. 40, Issue 4). https://doi.org/10.1111/1467-6486.00361

Littler, C. R. (1978). Understanding Taylorism. *The British Journal of Sociology*, *29*(2). https://doi.org/10.2307/589888

Majchrzak, A., Markus, M. L., & Wareham, J. (2016). Designing for Digital Transformation. *MIS Quarterly*, *40*(2).

Martin, K. (2013). Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online. *First Monday*. https://doi.org/10.5210/fm.v18i12.4838

Martin, K. (2016a). Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop? *Information Society*, *32*(1), 51–63. https://doi.org/10.1080/01972243.2015.1107166

Martin, K. (2016b). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, *137*(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Martin, K. (2018). The penalty for privacy violations: How privacy violations impact trust online. *Journal of Business Research*, *82*, 103–116. https://doi.org/10.1016/j.jbusres.2017.08.034

Martin, K. (2020). Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms. *Business Ethics Quarterly*, *30*(1). https://doi.org/10.1017/beq.2019.24

Martin, K. E. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics*, *111*(4), 519–539. https://doi.org/10.1007/s10551-012-1215-8

Martin, K. E. (2015). Ethical Issues in the Big Data Industry. *MIS Quarterly Executive*, *2015*(June), 74–87. https://doi.org/1540-1960

Massa, F. G. (2017). Guardians of the Internet: Building and Sustaining the Anonymous Online Community. *Organization Studies*, *38*(7). https://doi.org/10.1177/0170840616670436

McAfee, A., & Brynjolfsson, E. (2012). Big Data. The management revolution. *Harvard Buiness Review*. https://doi.org/10.1007/s12599-013-0249-5

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2), 2053951720948087. https://doi.org/10.1177/2053951720948087

Miller, S., & Weckert, J. (2000). Privacy, the Workplace and the Internet. *Journal of Business Ethics*. https://doi.org/10.1023/A:1006232417265

Morozov, E. (2013). To save everything, click here : the folly of technological solutionism / Evgeny Morozov. *To Save Everything, Click Here : The Folly of Technological Solutionism*.

Morton, A. D. (2007). Waiting for Gramsci: State formation, passive revolution and the international. *Millennium: Journal of International Studies*, *35*(3). https://doi.org/10.1177/03058298070350031301

Muellerleile, C., & Robertson, S. L. (2018). Digital Weberianism: Bureaucracy, Information, and the Techno-rationality of Neoliberal Capitalism. *Indiana Journal of Global Legal Studies*, *25*(1). https://doi.org/10.2979/indjglolegstu.25.1.0187

Muldoon, J. (2022). *Platform Socialism: how to reclaim our digital future from Big Tech*. London: Pluto Press.

Mumby, D. K. (2005). Theorizing resistance in organization studies: A dialectical approach. *Management Communication Quarterly*, *19*(1), 19–44.

Mumby, D. K., Thomas, R., Martí, I., & Seidl, D. (2017). Resistance Redux. *Organization Studies*, *38*(9), 1157–1183. https://doi.org/10.1177/0170840617717554

Nissenbaum, H. (2004). Privacy as contextual integrity. *Wash. L. Rev.* https://doi.org/10.1109/SP.2006.32

Obar, J. A. (2015). Big Data and The Phantom Public: Walter Lippmann and the fallacy of data privacy self-management. *Big Data and Society*. https://doi.org/10.1177/2053951715608876

Obar, J. A. (2020). Sunlight alone is not a disinfectant: Consent and the futility of opening Big Data black boxes (without assistance). In *Big Data and Society*. https://doi.org/10.1177/2053951720935615

Ometto, M. P., Gegenhuber, T., Winter, J., & Greenwood, R. (2019). From Balancing Missions to Mission Drift: The Role of the Institutional Context, Spaces, and Compartmentalization in the Scaling of Social Enterprises. *Business and Society*, *58*(5). https://doi.org/10.1177/0007650318758329

Ossewaarde, M., & Reijers, W. (2017). The illusion of the digital commons: 'False consciousness' in online alternative economies. *Organization*, *24*(5), 609–628. https://doi.org/10.1177/1350508417713217

Parida, V., Sjödin, D., & Reim, W. (2019). Reviewing literature on digitalization, business model innovation, and sustainable industry: Past achievements and future promises. In *Sustainability (Switzerland)* (Vol. 11, Issue 2). https://doi.org/10.3390/su11020391

Park, E. A. (2017). Why the networks can't beat Netflix: speculations on the US OTT Services Market. *Digital Policy, Regulation and Governance* , *19*(1). https://doi.org/10.1108/DPRG-08-2016-0041

Parsons, C. (2019). The (In)effectiveness of Voluntarily Produced Transparency Reports. *Business and Society*. https://doi.org/10.1177/0007650317717957

Peticca-Harris, A., DeGAMA, N., & Ravishankar, M. N. (2020). Postcapitalist precarious work and those in the 'drivers' seat: Exploring the motivations and lived experiences of Uber drivers in Canada. *Organization*, *27*(1), 36–59.

Rabindranath, M., & Kapil, S. (2014). Social Media and the Arab Spring. *Media Watch*. https://doi.org/10.15655/mw/2015/v6i1/55438

Rainie, L., Kiesler, S., & Kang, R. (2013). Anonymity, privacy, and security online. In *Pew Research Center*.

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. *Big Data and Society*, *6*(1). https://doi.org/10.1177/2053951718820549

Schade, F. (2023). Dark Sides of Data Transparency: Organized Immaturity After GDPR? *Business Ethics Quarterly*. https://doi.org/10.1017/beq.2022.30

Seeck, H., Sturdy, A., Boncori, A. L., & Fougère, M. (2020). Ideology in Management Studies. *International Journal of Management Reviews*, *22*(1). https://doi.org/10.1111/ijmr.12215

Simsek, Z., Li, N., & Huang, J. L. (2022). Turbocharging Practical Implications in Management Studies. Journal of Management, 48(5), 1083–1102. https://doi.org/10.1177/01492063211040562

Steinberg, M. (2022). From Automobile Capitalism to Platform Capitalism: Toyotism as a prehistory of digital platforms. *Organization Studies*, *43*(7). https://doi.org/10.1177/01708406211030681

Taskin, L., Courpasson, D., & Donis, C. (2022). Objectal resistance: The political role of personal objects in workers' resistance to spatial change. *Human Relations*, 00187267211067142.

Thatcher, J., O'Sullivan, D., & Mahmoudi, D. (2016). Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space*, *34*(6), 990–1006. https://doi.org/10.1177/0263775816633195

The Economist. (2017). The world's most valuable resource is no longer oil, but data. *The Economist*.

Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, *28*(1), 8–25.

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society*. https://doi.org/10.1177/0270467607311484

United Nations Conference on Trade and Development. (2023). *Data Protection and Privacy Legislation Worldwide*. UNCTAD.

Van Dijck, J. (2020). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media and Society*. https://doi.org/10.1177/1461444820940293

Van Lent, W., Islam, G., & Chowdhury, I. (2021). ‘Civilized Dispossession’: Corporate accumulation at the dawn of modern capitalism. *Organization Studies*, 01708406211026127.

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/J.JSIS.2019.01.003

von Krogh, G. (2018). Artificial Intelligence in Organizations: New Opportunities for Phenomenon-Based Theorizing. *Academy of Management Discoveries*, *4*(4). https://doi.org/10.5465/amd.2018.0084

Walker, M., Fleming, P., & Berti, M. (2021). ‘You can’t pick up a phone and talk to someone’: How algorithms function as biopower in the gig economy. *Organization*, *28*(1), 26–43. https://doi.org/10.1177/1350508420978831

West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & Society*, *58*(1), 20–41.

Whelan, G. (2013). Corporate constructed and dissent enabling public spheres: Differentiating dissensual from consensual corporate social responsibility. *Journal of Business Ethics*, *115*(4). https://doi.org/10.1007/s10551-013-1823-y

Whelan, G. (2019). Born Political: A Dispositive Analysis of Google and Copyright. *Business and Society*. https://doi.org/10.1177/0007650317717701

Wielki, J. (2015). The social and ethical challenges connected with the big data phenomenon . *Polish Journal of Management Studies*, *11*(2), 192–202. http://www.scopus.com/inward/record.url?eid=2-s2.0-84935088081&partnerID=40&md5=22222f72d0af8c175dee96d9ccdd9426

Wilhoit, E. D., & Kisselburgh, L. G. (2015). Collective Action Without Organization: The Material Constitution of Bike Commuters as Collective. *Organization Studies*, *36*(5). https://doi.org/10.1177/0170840614556916

Ybema, S., & Horvers, M. (2017). Resistance Through Compliance: The Strategic and Subversive Potential of Frontstage and Backstage Resistance: *Http://Dx.Doi.Org/10.1177/0170840617709305*, *38*(9), 1233–1251. https://doi.org/10.1177/0170840617709305

Youn, S. (2009). Determinants of Online Privacy Concern and Its Influence on Privacy Protection Behaviors among Young Adolescents. *Journal of Consumer Affairs*. https://doi.org/10.1111/j.1745-6606.2009.01146.x

Zahra, S. A., & Newey, L. R. (2009). Maximizing the impact of organization science: Theory-building at the intersection of disciplines and/or fields. Journal of management studies, 46(6), 1059-1075.

Zanoni, P., Contu, A., Healy, S., & Mir, R. (2017). Post-capitalistic politics in the making: The imaginary and praxis of alternative economies. In *Organization* (Vol. 24, Issue 5, pp. 575–588). SAGE Publications Sage UK: London, England.

Zott, C., Amit, R., & Massa, L. (2011). The business model: Recent developments and future research. In *Journal of Management* (Vol. 37, Issue 4). https://doi.org/10.1177/0149206311406265

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs.