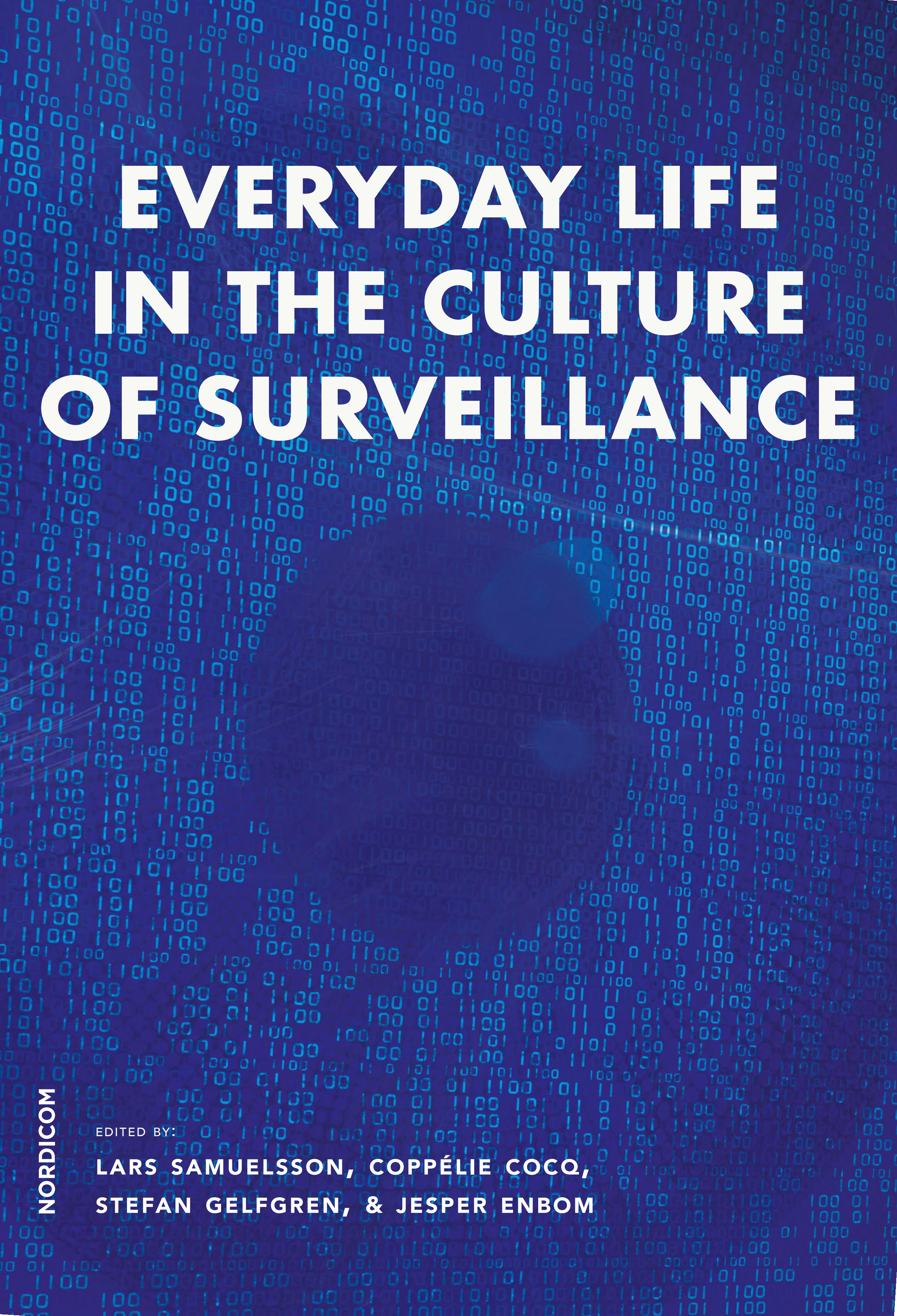

EVERYDAY LIFE IN THE CULTURE OF SURVEILLANCE

EDITED BY:

LARS SAMUELSSON, COPPÉLIE COCQ,
STEFAN GELFGREN, & JESPER ENBOM

NORDICOM

EVERYDAY LIFE
IN THE CULTURE OF
SURVEILLANCE

Everyday Life in the Culture of Surveillance
Lars Samuelsson, Coppélie Cocq,
Stefan Gelfgren, & Jesper Enbom (Eds.)

ISBN (PRINT): 978-91-88855-72-5
ISBN (PDF): 978-91-88855-73-2

This work is Open Access and available to read free of charge and without registration requirement at www.nordicom.gu.se/en/publications/everyday-life-culture-surveillance

DOI: 10.48335/9789188855732

CITE THIS WORK:
Samuelsson, L., Cocq, C., Gelfgren, S., & Enbom, J. (Eds.). (2023). Everyday life in the culture of surveillance. Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732

PUBLISHED BY:
Nordicom, University of Gothenburg
Box 713
SE 405 30 Göteborg, Sweden

www.nordicom.gu.se/en

COVER BY: Karin Andén

EVERYDAY LIFE IN THE CULTURE OF SURVEILLANCE

EDITED BY:

LARS SAMUELSSON, COPPÉLIE COCQ,
STEFAN GELFGREN, & JESPER ENBOM

Contents

Preface

In November 2014, The Faculty of Arts and Humanities at Umeå University, Sweden, invited its researchers to a two-day research workshop in the city of Örnsköldsvik, about a hundred kilometers south of Umeå. During these days, groups formed around different themes suggested by participants as interesting convergence points for researchers from various humanities subjects. One of these themes, proposed by Stefan Gelfgren, was the issue of contemporary surveillance and the role and impact it has in people's lives. Surveillance is a phenomenon that saturates everyday life in modern societies, and researchers from different humanities disciplines could be expected to find interesting and important angles to this topic. That turned out to be the case!

In the wake of the workshop, an interdisciplinary group took shape with the initial aim of applying for seed money from the faculty for writing a research application focusing on "soft surveillance" – the kind of surveillance we are exposed to when we seemingly voluntarily share our personal information, not least through our online activities. At this point, the group consisted of five researchers: Stefan Gelfgren, Coppélie Cocq, Jesper Enbom, Anna Johansson, and Lars Samuelsson. The faculty approved the seed money and in early 2016 the group went on a short writing retreat to the village Vännäs outside of Umeå to work on their application. It was submitted in March 2016 to Marcus and Amalia Wallenberg Foundation (MAW). The proposed research project got the title "iAccept: Soft surveillance – between acceptance and resistance", and its aim was expressed as follows: "to investigate the tension between, on the one hand, contemporary forms of soft surveillance and the rationales provided by surveillance agents, and, on the other, the way individual users approach, understand, and negotiate the impact of soft surveillance in their everyday life".

In December the same year the application was granted funding from MAW, and the real work could begin. Among the anticipated outcomes of the

Samuelsson, L., Cocq, C., Gelfgren, S., & Enbom, J. (2023). Preface. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 6–8). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-p

project was a book with the purpose of summing up important results and collecting relevant contributions from various humanities scholars (broadly conceived), illuminating different angles of the topic. The plan was to initiate the work with the book in relation to an international workshop, to be carried out within the framework of the iAccept-project. But like so many other things, the project was both delayed and had to be partly redesigned due to the Covid-19 pandemic. The workshop plans had to be abandoned, and instead we settled on either an anthology or a special journal issue based on an open call for chapters or papers. An advantage with this alternative was the possibility to reach out more widely to researchers from various disciplines and in different parts of the world. We presented our proposal to Nordicom, at the University of Gothenburg, with whom we had published an overview article earlier in the project. To our delight, Nordicom seized on the idea, and suggested we go for an anthology rather than a special issue – a choice that we are now very happy about.

In April 2021, the call for chapters was published on Nordicom's website and spread in various channels. Over the following months, we received a variety of interesting proposals, nine of which made it to the final book. It is our conviction that together these chapters make an important contribution to the field of surveillance studies – highlighting cultural and ethical perspectives on everyday surveillance, with a focus on the Nordic countries. We want to thank the authors of the chapters for their contributions to, and engagement with, the book; for their collaborative spirit and the work they have put into their chapters. Without them there would not have been any book.

The Nordicom staff has been fantastic – supportive and extremely helpful throughout the project. In particular, we want to thank scientific editor Johannes Bjerling, who has provided crucial comments and suggestions to each chapter, as well as regarding the book project as a whole; managing editor Josefine Bové, who has assisted us with practical matters and given valuable input; manuscript editor Kristin Clay, for her thorough and efficient editing of all the chapters; graphic designer Karin Andén for her layout of the book; and communications officer Sara Stenkvist, who administrates the marketing and communication of the book. In addition, we want to express our gratitude to the anonymous reviewers of the chapters for their important contribution to the quality of the book.

Working with this anthology – collaborating with the authors and the publisher – has been a pleasure. It is hard to imagine a smoother process – from the initial contact with the publisher and the online meetings with the authors, to the final stages of putting everything together in its final shape. We are very satisfied with the result!

We also want to take the opportunity to acknowledge the previous project members of iAccept: Anna Johansson – who took part in designing the project and applying for its funding, but who unfortunately (from our perspective) had to leave it early due to a change of job – and Peter Bennesved, who joined the project as assistant professor during six months in 2021 to contribute with a valuable historical perspective.

This anthology is an outcome of the research project "iAccept: Soft surveillance – between acceptance and resistance" (MAW 2016.0092), funded by the Marcus and Amalia Wallenberg Foundation. We are grateful to MAW for the financial support that enabled both the project and the book. As we write this preface, we have just been awarded research funding for a new project (again from MAW): "Data Is the New Oil (DINO): Digital transformation – negotiating societal benefits and personal integrity". With this project, we will further investigate the digital transformation of society and what it means to the people who live in the midst of this development – in the midst of a surveillance culture.

Lars Samuelsson, Coppélie Cocq, Stefan Gelfgren, & Jesper Enbom

Umeå, January 2023

Introduction

The complex web of everyday surveillance

STEFAN GELFGREN,[I] COPPÉLIE COCQ,[II] LARS SAMUELSSON,[I] & JESPER ENBOM[III]

[I] DEPARTMENT OF HISTORICAL, PHILOSOPHICAL AND RELIGIOUS STUDIES, UMEÅ UNIVERSITY, SWEDEN

[II] HUMLAB, UMEÅ UNIVERSITY, SWEDEN

[III] DEPARTMENT OF CULTURE AND MEDIA STUDIES, UMEÅ UNIVERSITY, SWEDEN

ABSTRACT

The possibilities to surveil people have increased and been further refined with the implementation of digital communication over the last couple of decades, and with the ongoing process of digital transformation, surveillance can now go in any direction, leaving a label such as "surveillance state" somewhat outdated. Corporations and governmental organisations may surveil people, people may surveil each other, and surveillance may take place in subtle ways that are difficult for the surveilled to detect. In David Lyon's terms, we are living in a "culture of surveillance", a culture that surrounds and affects our everyday life. Today, it is of utmost relevance to study people's attitudes, motives, and behaviours in relation to the fact that we live in a culture of surveillance. This includes the need for cultural and ethical perspectives to understand and nuance contemporary discussions on surveillance, not least in the highly digitalised context of the Nordic countries. The chapters in this anthology address these issues from a variety of disciplinary and theoretical frameworks.

KEYWORDS: surveillance, surveillance culture, digitalisation, data-driven, digital transformation

Gelfgren, S., Cocq, C., Samuelsson, L., & Enbom, J. (2023). Introduction: The complex web of everyday surveillance. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 9–20). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-i

Introduction

Surveillance is a multifaceted concept, usually connected to issues such as power and control, directed from societal authorities in order to control citizens. Historical discussions have usually drawn upon the Benthamian concept of the panopticon, which was adapted and further developed in Michel Foucault's (1979) seminal work *Discipline and Punish* (original title, *Surveiller et punir*, published in 1975). Foucault claimed that in modern society (18th century onwards), citizens have internalised the eye of the state (a theme also popularised in and through George Orwell's *Nineteen Eighty-Four*). Today, the possibilities to surveil people have been further refined with the implementation of digital communication, and the discussion has evolved from a unilateral focus on top-down surveillance to a broader understanding, where surveillance occurs between different actors and in different spheres of society – a development supported and enhanced by technological developments.

In a contemporary common-sense understanding, surveillance is a "close watch kept over someone or something" (Merriam-Webster, n.d.) or the "monitoring of behavior, many activities, or information for the purpose of information gathering, influencing, managing or directing" (Wikipedia, n.d.). This common-sense understanding of surveillance is something this book adheres to, but we aim to develop it further. In this book, we focus on one rather specific form of surveillance: surveillance related to the data-saturated society we all live in and must relate to. Hence, a concept central to the book is *online* surveillance, which – in line with our understanding of surveillance – is understood broadly: any collection of any kind of information online about persons may count as online surveillance (Leckner, 2018; compare with Fuchs, 2017; Lyon, 2014). This form of surveillance saturates modern life for most people and may go in any direction – companies and governmental organisations may surveil people, people may surveil each other, and surveillance may take place in subtle ways that are difficult for the surveilled to detect. In David Lyon's (2017, 2018) terms, we are living in a "culture of surveillance", a culture that surrounds and affects our everyday life. By studying everyday life in the culture of surveillance, this book contributes to the understanding of the time we live in. While the book is not restricted to investigations in the Nordic countries, they provide its central focus.

The aim of this book is to study people's attitudes, motives, and behaviours in relation to the fact that we live in a culture of surveillance, where personal data is gathered and analysed on a daily basis. We thus want to emphasise the need for cultural and ethical perspectives to understand and nuance contemporary discussions on surveillance, here manifested through compiling an anthology with contributions by scholars from a variety of disciplines, such as philosophy, media and communication studies, sociology and digital humanities, among others.

This anthology is an outcome of a research project “iAccept: Soft Surveillance – Between Acceptance and Resistance”, the aim of which was to investigate the ways individuals and collectives working with data in Sweden (laypeople, researchers, and communication officers at political parties) approach, understand, and negotiate the impact of surveillance in their everyday lives. Such questions are represented in the contributions, but we have also broadened the scope to include more societal and cultural perspectives in a larger geographical (primarily Nordic) context, thus using the concept of surveillance culture as a point of departure.

Contextual framework

The concept of and the practices regarding a culture of surveillance have emerged due to different circumstances during the last decades. More specifically, the current situation has emerged since approximately 2000, following the distribution and implementation of the Internet as a high-speed communication system on a large scale; the so-called war on terror following the 11 September terrorist attacks in 2001; the technological development of smartphones, social media, and wearables; and the ever-growing capacity to generate, store, coordinate, and analyse data. While surveillance practices were previously done by, and associated with, discernible actors, often “from above” and directed toward potential threats (individuals or smaller collectives) to protect the state or specific interests, surveillance is today ubiquitous and performed by a variety of actors – ranging from state authorities, commercial interests, welfare institutions, to our fellow friends – with different purposes. We return to this development below, when elaborating the emergence of a culture of surveillance.

Today, data – information – is both a curse and a blessing. Data is all around us, and we continuously use and generate data through our use of social media platforms, electronic devices, banking services, and welfare systems. On the one hand, the abundance of data gives the opportunity to discern patterns, to see how different data relate, and thus to analyse and predict current and future behaviour to coordinate and optimise resources and competences for the greater good. On the other hand, the very same data can be used to surveil us and to monitor our behaviours: same data, same phenomenon, but with different purposes and outcomes, depending on who is doing the act of surveillance and with what intention. What can be seen as legitimate and motivated by a benevolent purpose can also be seen as intrusive and violating personal integrity – depending on personal outlook and the intentions behind the surveillance. This is something we can all relate to.

Let us begin by giving a contemporary example where surveillance has surfaced as a pressing and relevant issue and which highlights the tension between perceived possibilities and threats on both individual and societal levels. As we write this introduction (October 2022), we hope to put the

Covid-19 pandemic behind us, but we all remember the different restrictions and the discussions on how to stop the spread of the virus (which varied from country to country). One suggestion, implemented in some countries, was to keep track of all contaminated people through a database and a smartphone app that gave a warning if a contaminated person was in contact with a non-contaminated person. Your smartphone could also be used as a device to track your own movement and ensure that you did not leave your designated personal quarantine. Health data and place data, in this way, can be used to protect people from Covid-19, but at the possible expense of personal integrity. For some, this is considered a price worth paying to stop the pandemic, but it can also be seen as too high a price to pay in terms of integrity. This issue was discussed (quite heatedly, from time to time) through various media outlets – in traditional media and in the so-called alternative media, often on and through social media platforms (see, e.g., Andersson Schwarz et al., 2020; Westerberg, 2020).

To add another layer to this controversy, social media platforms such as Facebook and Twitter, and also Google, began moderating and checking posted content related to Covid-19, which, on the one hand, was seen as relevant and necessary in order to prevent the spreading of misinformation, but on the other, could be seen as intrusive and biased – again, all depending on individual beliefs and opinions. Proponents of restrictions were confronted by those against restrictions, and vice versa, where the tech companies – through the data we share – could monitor and steer the discussion through its algorithms. Whether this is good or bad is not our current question, but we note how the use of data can both mobilise and polarise discussions and people – against each other, and in relation to a public debate. Here, people are surveilled but are also surveillers, through a web of intertwining relations between authorities, media, tech companies, and fellow citizens, affecting both the public and personal spheres, and affecting behaviour and intellectual discourse. This is only one example; the chapters in this volume elaborate on additional examples of this phenomenon, adding complexity and concretisation to the culture of surveillance.

The process toward increasing surveillance is present, and the possibilities of increased access to data are often praised by, for example, the United Nations, OPEC, the European Union, and national governments, under the term of digital transformation. Digital transformation is deemed beneficial for health research, resource optimisation, democratisation, and more. On an everyday micro level, people are affected by this process and must relate to it, mentally and practically.

Toward a culture of surveillance

The ubiquitous and everyday aspect of surveillance calls for cultural and ethical perspectives on surveillance, in order to understand the complexity of being a human in the culture of surveillance. By referring to a culture of surveillance, we here adhere to and draw on what Torin Monahan (2011: 495) referred to as "surveillance as cultural practice", a practice that involves the study of social practices in different cultural contexts, "likely to try to comprehend people's engagement with surveillance on their own terms" (Monahan, 2011: 495).

However, even though this ubiquitous surveillance situation is noticeable – and currently changing how we all live our lives – it has been difficult to empirically study everyday life in a digitally permeated society, as discussed by Ball, Haggerty, and Lyon (2012), and further developed by, for example, Green and Zurawski (2015), and Eley and Rampton (2020), who started to take more of an anthropological or ethnographic approach to surveillance. Also, Bucher (2017: 31) noted the lack of empirical studies of the realities of a digital everyday life: "there is not much existing research on the ways in which people experience and perceive algorithms as part of their everyday life". Hence, this book aims to study people's attitudes, motives, and behaviours and will allow us to capture and interpret practices and ideas in relation to the culture of surveillance.

Our point of departure is David Lyon's concept "culture of surveillance" (2018), or "surveillance culture" (2017), which he uses to describe and understand how surveillance affects us all:

> [Surveillance] is no longer merely something external that impinges on our lives. It is something that everyday citizens comply with – willingly and wittingly, or not – negotiate, resist, engage with, and, in novel ways, even initiate and desire. From being an institutional aspect of modernity or a technologically enhanced mode of social discipline or control, it is now internalized and forms part of everyday reflections on how things are and of the repertoire of everyday practices. (Lyon, 2017: 825).

If surveillance is intertwined into all our lives, creating the culture in which we live, as Lyon (and Monahan, 2011) claims, then this calls for research from humanist and cultural perspectives, meaning that scholars from fields such as cultural studies, philosophy, history, language studies, and so on are urged to bring their perspectives and interpretations when trying to understand "the culture of surveillance". What does it mean for people to live in, and have to deal with, a surveillance culture? How do people handle this situation – in terms of compliance, resistance, or ignorance? How has this changed through time? What implications does surveillance have on personal integrity and human rights? These are questions that scholars from aforementioned fields are well apt to discuss and provide answers to.

From surveillance state to surveillance culture

The development towards a data-saturated society during the last couple of decades has meant that a label such as "surveillance state" (Balkin, 2008) seems somewhat outdated. Balkin brings forward important cautions regarding the increasing government use of surveillance and data mining in the US. Although he points out how private corporations are more involved in surveillance, for example, regarding tastes and preferences among customers, Balkin's focus is on top-down surveillance by different government agencies. When Balkin observes the development towards intertwined public and private surveillance, he tends to view the latter as a dangerous supplement of the former. Instead, we need to understand how the traditional notion of surveillance as something carried out by government agencies against the citizens needs to be amended to accommodate a more pervasive form of surveillance. The possibilities to use data to surveil individuals by government agencies, for example, through policing and the provision of social services, have been refined together with the implementation of digital communication.

Instead of the Orwellian dystopia, in which the individual is monitored by the state, surveillance today permeates everyday life. Haggarty and Ericsson (2000: 606) use the concept of "surveillant assemblage" to describe how human bodies are abstracted from their spatial settings and separated into a multitude of data flows. Information about individuals is then collected from these flows and reassembled as "data doubles", which in turn are scrutinised and used by a range of actors. This development was observed as early as the 1980s by Clarke (1988), when he introduced the concept of "dataveillance". He defined it as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988: 499). According to van Dijck (2014), this dataveillance differs from traditional surveillance, because surveillance is used for a specific purpose, while dataveillance is the continuous tracking of data *without* clear purposes. With the ever-growing possibilities of data collection and data analyses, dataveillance penetrates every aspect of our culture and everyday life.

For Zuboff (2015), Big Data is the central component of a new logic of accumulation that she calls "surveillance capitalism". The new global data collection has created new monetisation opportunities due to the ways large corporations, especially tech firms such as Google, can predict and modify human behaviour. Zuboff stresses how the use of Big Data by corporations and other organisations – in other words, dataveillance – should be seen not as an inevitable technology effect but as the intentional creation of the industry (see Zuboff, 2019).

The development towards ever increasing collection of data and surveillance by corporations and government agencies has also contributed to the spread of counter-surveillance among marginalised groups and social justice activists. An important part of this work has constituted "sousveillance", the use of the new surveillance technologies to surveil those in power and hold them accountable (Mann et al., 2003). Not least has this taken the form of monitoring police interventions using video, audio. and even specific smartphone apps (Bärbel, 2020). Borradaile and Reeves (2020), though, highlighted how even these protest movements become incorporated in surveillance capitalism, due to the ways they rely on major tech and communications firms for both hardware and software.

The concept of a culture of surveillance reveals how surveillance is something we nowadays live in, and which we all, on a daily basis and more or less continuously, must negotiate with. This concept is developed from Lyon's earlier concept of surveillance society (where surveillance still has discernible actors and a top-down perspective), broadening the scope to include non-discernible actors and the all-encompassing nature of surveillance in contemporary society:

> Once thought of mainly as the world of private investigators, police and security agencies, the means of surveillance now also flow freely through many media into the hands of the general public. This has helped to create an emerging surveillance culture – the everyday webs of social relations, including shared assumptions and behaviours, existing among all actors and agencies associated with surveillance. (Lyon, 2018: 30)

This culture is significant for our present day and has grown out of technical achievements (social media, Internet access, and portable Internet-connected devices), the digital transformation of society and businesses, and events such as 9/11, the following war on terror (which grew out of security concerns), the Cambridge Analytica affair, and so on. Lyon himself defines culture in line with Raymond Williams (1958) as a "whole way of life", that is, a complex web of practicalities, norms, and ideas that we all are embedded in.

In order to understand and study how people relate to, and negotiate, the culture of surveillance, Lyon (2018) divides the culture into the related concepts of surveillance imaginaries (what people think about and are influenced by) and surveillance practices (what people *do* in relation to their imaginaries concerning surveillance). Our imaginaries are formulated by public debate, science, law, popular culture, and so on, and constitute a framework – a discourse – to which we respond in different ways.

The Nordic region as a context

While surveillance has a global impact and affects societies all around the world, this anthology focuses on surveillance in the Nordics. In many ways, the Nordics are an exception in the world, well-illustrated by the Inglehart-Welzel World Cultural Map (World Values Survey, 2022), where the Nordic countries are shown to favour self-expression and non-traditional and secular values.

In the 2021 report from The Swedish Internet Foundation (2021: para. 1–3), Sweden is described as,

> a society that is largely digitised and where online life for most people is a natural part of work, school, and spare time. Of the entire population in Sweden, 9 out of 10 use the internet every day [and] 9 out of 10 use various public e-services provided by, for example, The Swedish Tax Agency, The Swedish Social Insurance Agency, healthcare or the library.

This high degree of connectivity and extensive use of the Internet and digital services is similar in the other Nordic countries, where the development of digital infrastructures is a process that has been going on for decades. The Nordics were early adopters of the Internet and digital technologies, and several social projects supported the implementation of computers and connectivity at home and in work life. It is important to note that Internet and social media use are not confined to young and middle-aged people. In Sweden, for example, approximately 80 per cent of 60–80-year-olds use social media platforms at least once a week (The Swedish Internet Foundation, 2021). This implies that we do not only find a high degree of connectivity with high-speed Internet, but also a high level of digital literacy in the Nordic societies. Therefore, this anthology presents a digital reality that might illustrate a near future for other countries of Europe and in the world.

Another aspect specific to the Nordic countries that we find key to understanding the advancement and digitalisation of our societies – and, consequently, core to understanding the surveillance culture – is the fact that Sweden, Norway, Finland, and Denmark are all high-trust nations, something that is confirmed by the results of, for example, European Value Surveys and the World Happiness Report, among others (see, e.g., Martela et al., 2020). Previous research about attitudes to surveillance (e.g., Denemark, 2012; Svenonius & Björklund, 2018) indicates that social and institutional trust plays a key role in the acceptance of surveillance. But also, research shows the key role of privacy concerns, and not least how cultural origin must be taken into account in order to understand attitudes to surveillance (Svenonius & Björklund, 2018).

Content of the book

In addition to this introduction and a concluding chapter, this volume consists of nine contributions that together cover a wide range of themes and content, ranging from general theoretical issues pertaining to life in a culture of surveillance, to investigations of particular surveillance aspects and contexts, including studies focusing on the Nordic countries.

The first four chapters centre around different digital practices deeply intertwined with everyday life – practices which all involve a relation to data collection, data analysis, and ultimately, to surveillance.

In Chapter 1, "Being played in everyday life: Massive data collection on mobile games as part of ludocapitalist surveillance dispositif", Maude

Bonenfant, Alexandra Dumont, and Laura Iseut Lafrance St-Martin discuss and problematise everyday surveillance in mobile gaming, drawing attention to associated ethical considerations and examining how gamers are involved in the trivialisation of this surveillance practice. The authors thoroughly explain the mechanisms and purposes of data collection, thus providing a useful background to the subsequent chapters.

The ethical dimension of data collection is further elaborated in Chapter 2, "To be a face in the crowd: Surveillance, facial recognition, and a right to obscurity", where Shawn Kaplan scrutinises the ethics of video surveillance, particularly the need to reconsider our guiding principles in this area considering the emergence of facial recognition technology. Kaplan reveals the multifaceted ethical dimension of video surveillance (and surveillance in general), discussing the practical need to articulate a novel right to obscurity, in addition to the commonly acknowledged right to privacy, in order to protect the interests pertinent to liberal democracies.

In Chapter 3, "To see and be seen: Gynaeopticism and platform surveillance in influencer marketing", Johanna Arnesson and Eric Carlsson deal with surveillance practices in the digital marketing industry by exploring what types of surveillance are present in the influencer industry. Based on empirical examples from Sweden, with special focus on a group of successful influencers in the lifestyle and fashion genre, Arnesson and Carlsson discuss how different dimensions of surveillance – self, peer, and top-down – are manifested, exploited, and contested.

Chapter 4, "Tracking (in)fertile bodies: Intimate data in the culture of surveillance", centres around the practice of fertility self-tracking, through which women, with the help of digital tracking devices and mobile apps, track symptoms and signs relating to their menstrual cycle. Based on interviews with eleven women (ten Swedish and one Finnish) who engage in fertility self-tracking, Kristina Stenström investigates the participants' motives for engaging in fertility self-tracking and their understandings of the intimate surveillance involved.

Although the Nordic context is apparent in the latter two chapters, the following four chapters turn attention to the conditions in the Nordics more directly. Three of them focus on how young people perceive, relate to, and think about privacy and online surveillance in different contexts, looking at Sweden, Finland, and Norway, respectively, whereas one is more general regarding age, and discusses online surveillance in a Danish context.

In Chapter 5, "It all depends on context: Danes' attitudes towards surveillance", Rikke Frank Jørgensen proceeds from the Danish Values Survey in her analysis of Danish citizens' views on three categories of state surveillance – CCTV surveillance in public places; monitoring of information exchanged on the Internet; and the collection of information about citizens without their knowledge – and she explores how and why their attitudes to these types of surveillance differ.

In Chapter 6, “Accepting or rejecting online surveillance: The case of Swedish students”, Lars Samuelsson draws on a survey of approximately 1,000 Swedish students to discuss how young Swedes think about the justifiability of online surveillance. He considers three conditions that might increase the acceptance of such surveillance – that surveillance results in personal benefits; that it has been consented to; and that society can benefit from it – and discusses to what extent they seem to affect the students' acceptance of being surveilled.

Chapter 7, “Smartphone privacy: Finnish young people's perceptions of privacy regarding data collected when using their mobile devices”, turns attention to Finnish teenagers' experiences of privacy in relation to their use of smartphones. Adopting a mixed-methods approach combining concept mapping, Q-sorting, and in-depth interviews, Liisa A. Mäkinen and Johanna Junnila examine what kinds of factors are meaningful for young people when considering phone-related privacy, and how their desires for privacy vary in terms of different audiences.

Chapter 8, “Omnipresent publicness: Social media natives and protective strategies of non-participation in online surveillance”, focuses on the question of how young people in Norway, accustomed to online spaces as part of social life, evaluate and use social media as private and public spaces. Drawing on eleven in-depth interviews with Norwegian young adults, Luise Salte investigates experiences and strategies concerning privacy and online surveillance of social media natives in relation to their use of social media platforms.

In the final contribution to the book, Chapter 9, “Kant's ethics in the age of online surveillance: An appeal to autonomy”, we return to general theoretical aspects of surveillance. Here, Casey Rentmeester puts surveillance in a philosophical context, analysing the contemporary paradigm of online surveillance by unpacking the power dynamics involved in online surveillance. Utilising Immanuel Kant's ethics and political philosophy, Rentmeester argues that respect for personal autonomy must be at the forefront of the ethics of online surveillance. In addition to this argument, Rentmeester also introduces various philosophical aspects of surveillance, drawing attention to the importance of attending to such theoretical aspects of the issue.

Conclusion

These nine chapters together illustrate and emphasise multiple aspects of everyday surveillance – this culture of surveillance that charaterises contemporary societies. In this anthology, researchers from a variety of disciplines shed light on the complex web of surveillance culture, and perspectives from Denmark, Finland, Norway, and Sweden are complemented with perspectives on more general, and in some cases pressing, issues in relation to contemporary surveillance. In addition, these contributions point at the need for further research within and beyond the context of our Nordic societies, as discussed in the Afterword.

With this anthology, we hope to contribute to updating and broadening the field of surveillance studies by providing approaches from the humanities and social sciences. Together, the different contributions in this anthology highlight the need to critically discuss technological, social, political, and economical developments coming with the ongoing process toward the digital transformation of society that builds upon the collection, coordination, and interpretation of data. The concept of surveillance has indeed had negative connotations throughout history due to its top-down character, where the intention has been to control and domesticise people. The emergent culture of surveillance implies a need to nuance the picture. Sweeping ethical judgements about surveillance no longer come out as plausible given the multidirectedness of contemporary surveillance. The line between the surveiller and the surveilled is blurred, and we are all both objects and subjects of surveillance: We all both benefit from and are victimised by surveillance processes. This anthology is a contribution to the necessary conversation regarding our future in a data-driven society.

References

Andersson Schwarz, J., Ingram Bogusz, C., & Larsson, S. (2020, April 11). Pandemi-appar kan bli hot mot personliga integriteten [Pandemic-apps might be a threat to personal integrity]. *Dagens Nyheter*. https://www.dn.se/debatt/pandemi-appar-kan-bli-hot-mot-personliga-integriteten

Balkin, J. M. (2008). The constitution in the national surveillance state. *Minnesota Law Review*, *93*(1) 1–25.

Ball, K., Haggerty, K., & Lyon, D. (Eds.). (2012). *Routledge handbook of surveillance studies*. Routledge. https://doi.org/10.4324/9780203814949

Borradaile, G., & Reeves, J. (2020). Sousveillance capitalism. *Surveillance & Society*, *18*(2), 272–275. https://doi.org/10.24908/ss.v18i2.13920

Bucher, T. (2017). The algorithmic imaginary: Exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society*, *20*(1), 30–44. https://doi.org/10.1080/1369118X.2016.1154086

Bärbel, H. (2020). "Stay vigilant": Copwatching in Germany. *Surveillance & Society*, *18*(2), 280–283. https://doi.org/10.24908/ss.v18i2.13921

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, *31*(5), 498–512. https://doi.org/10.1145/42411.42413

Denemark, D. (2012). Trust, efficacy and opposition to anti-terrorism police power: Australia in comparative perspective. *Australian Journal of Political Science*, *47*(1), 91–113. https://doi.org/10.1080/10361146.2011.643163

Eley, L., & Rampton, B. (2020). Everyday surveillance, Goffman, and unfocused interaction, *Surveillance & Society*, *18*(2), 199–215. https://doi.org/10.24908/ss.v18i2.13346

Foucault, M. (1979). *Discipline and punish: The birth of the prison*. Vintage Books.

Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage. https://dx.doi.org/10.4135/9781446270066

Green, N., & Zurawski. N. (2015). Surveillance and ethnography: Researching surveillance as everyday life. *Surveillance & Society*, *13*(1), 27–43. https://doi.org/10.24908/ss.v13i1.5321

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622.

Leckner, S. (2018). Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and Internet surveillance in Sweden. *Northern Lights*, *16*(1), 113–132. https://doi.org/10.1386/nl.16.1.113_1

Lyon, D. (2014). The emerging surveillance culture. In A. Jansson, & M. Christensen (Eds.), *Media, surveillance and identity: Social perspectives* (pp. 71–90). Peter Lang. https://doi.org/10.3726/978-1-4539-1166-2

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 824–842. https://ijoc.org/index.php/ijoc/article/view/5527

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society*, *1*(3), 331–355. https://doi.org/10.24908/ss.v1i3.3344

Martela, F., Greve, B., Rothstein, B., & Saari, J. (2020). The Nordic exceptionalism: What explains why the Nordic countries are constantly among the happiest in the world. In J. F. Helliwell, R. Layard, J. D. Sachs, & J.-E. De Neve (Eds.), *World happiness report,* (pp. 128–145). Sustainable Development Solutions Network. https://worldhappiness.report/ed/2020/the-nordic-exceptionalism-what-explains-why-the-nordic-countries-are-constantly-among-the-happiest-in-the-world/

Merriam-Webster. (n.d.) Surveillance. In *Merriam-Webster.com dictionary*. Retrieved November 24, 2022, from https://www.merriam-webster.com/dictionary/surveillance

Monahan, T. (2011) Surveillance as cultural practice. *The Sociological Quarterly*, *52*(4), 495–508. https://doi.org/10.1111/j.1533-8525.2011.01216.x

Svenonius, O., & Björklund F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics*, *34*(2), 123–151. https://doi.org/10.1080/21599165.2018.1454314

The Swedish Internet Foundation. (2021). *Summary in English: The two sides of digital life*. https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2021/summary-in-english/

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12(*2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Westerberg, O. (2020, March 29). Övervakning används mot smittan i flera länder [Surveillance is used against the infection in several countries]. *Svenska Dagbladet/TT*. https://www.svd.se/a/RRebpd/covid-1984-overvakning-mot-smittan

Wikipedia. (n.d.) Surveillance. In *Wikipedia, the free encyclopedia*. Retrieved November 24, 2022, from https://en.wikipedia.org/wiki/Surveillance

Williams, R. (1958). *Culture and society 1780–1950*. Pelican Books.

World Values Survey. (2022). *The Inglehart-Welzel world cultural map – World values survery 7*. http://www.worldvaluessurvey.org

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of information technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.201

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

CHAPTER 1

Being played in everyday life

Massive data collection on mobile games as part of ludocapitalist surveillance dispositif

MAUDE BONENFANT, ALEXANDRA DUMONT,
& LAURA ISEUT LAFRANCE ST-MARTIN

DEPARTMENT OF SOCIAL AND PUBLIC COMMUNICATION, UNIVERSITÉ DU QUÉBEC À MONTRÉAL, CANADA

ABSTRACT
Surveillance in videogames is a well-known phenomenon. Designated as the fastest-growing sector of the videogame industry, mobile games – particularly free-to-play games – capitalise substantially on the collection of user data. Based on the promise of offering personalised gaming and advertising experiences, a vast quantity of data, including personal identifier and geolocation data, is acquired through players' mobile devices. While the information obtained may appear fragmented or invisible to players, they are consolidated in the hands of data brokers, resulting in a very lucrative economic sector. From this perspective, the practice of the mobile game, although innocuous at first consideration, raises essential ethical questions regarding the ludocapitalist surveillance dispositif established by this industry. In this chapter, we seek to problematise everyday surveillance in mobile gaming, explain how the videogame and marketing industries operate it, and examine gamers' ("ordinary" citizens) involvement in the banalisation of this massive data gathering.

KEYWORDS: ludocapitalism, mobile games, free-to-play, surveillance capitalism, Foucauldian dispositif

Bonenfant, M., Dumont, A., & Lafrance St-Martin, L. I. (2023). Being played in everyday life: Massive data collection on mobile games as part of ludocapitalist surveillance dispositive. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 21–44). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-1

Introduction

Journalist Julian Dibbell (2007) highlighted, in his article "The Life of the Chinese Gold Farmer", the growing connection between playing videogames and capitalism. This *New York Times* article describes the harsh living conditions of Chinese workers forced to play "massive multiplayer online games" for extended periods to acquire and then sell commodities over the Internet for profit. Dibbell argued that these modern-day sweatshops are symptoms of the capitalist ideology that aims to transform all human activities into instruments of wealth creation.

This economic framework blurs the distinction between labour and leisure by combining the principles of play (*ludus*) with contemporary capitalism. Known as ludocapitalism, this paradigm refers to,

> a hybrid or transitional moment of capitalism that describes its processes of commodity production and capital accumulation through reference to playing as a central concept of human activity and social organization, superseding the concept of work as the locus of rationality in traditional capitalist labour formations. (Jordan, 2014: 1)

Therefore, ludocapitalism considers the act of playing and generating wealth to be equivalent.

However, the capitalisation of players' activities is no longer the industry's primary monetisation method (Dibbell, 2007). Numerous game developers' revenue streams instead depend on collecting and selling consumer data, giving rise to new surveillance-based business models (Whitson, 2013). As such, surveillance capitalism centres primarily on commodifying personal data, with various industries – including marketing, insurance, and healthcare – using personal information to create profiles and infer customer behaviour (Zuboff, 2018). Zuboff described this economic and political shift as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales" (Zuboff, 2018: v). Accordingly, collecting personal data allows the prediction of behavioural patterns through increasingly sophisticated automated computer techniques, such as machine learning and artificial intelligence. Data exploitation aims to induce consumer behaviour by relying on the self-fulfilling prophecy (Merton, 1948) and manipulating desires through ever-increasingly precise individual profiling. Zuboff referred to this transition as a "dispossession by surveillance", an "exploitation of human nature", and a mechanism of social control that undermines freedom, democracy, and privacy. Furthermore, Zuboff (2015) argued that the well-known figure of Big Brother now takes the form of Big Other, a distributed power network for massive data collection.

In this chapter, we propose to articulate the principles of ludocapitalism and those of surveillance capitalism to introduce the new concept of surveillance ludocapitalism. While observable in the videogame industry, this concept rationale is most pervasive in the mobile game sector; rather than relying on retail profits, free-to-play mobile games depend substantially on the extensive collection of user data, including in-game behaviours and exchanges, which is algorithmically processed to develop targeted sales profiles (Bonenfant, 2021). The more individuals play, the more lucrative they become. Accordingly, a player's every action is subject to capitalisation, as autonomous algorithms log and extract each choice made in the game, the app store, and the smartphone itself. Despite its numerous negative implications for gamers and citizens, this business model based on surveillance capitalism grows year after year.

From this perspective, we explore everyday surveillance in mobile gaming, define how the videogame and marketing sectors use it, and examine gamers' participation as "ordinary" citizens in the trivialisation of this massive data gathering. The question guiding our research is: What are the conditions of possibility for widespread acceptance of large-scale surveillance through mobile gaming? We aim to provide a better understanding of the mobile games' economic, technical, psychological, semiotic, legal, and social context by focusing on participants' voluntary involvement and engagement within this everyday ludocapitalist surveillance dispositif, including, but not limited to, their "disciplinarisation" (Foucault, 1975). Our study contributes to the existing literature by schematising an industry traditionally challenging to investigate due to a lack of information and its structure's opacity.

First, we briefly explain the mobile game industry's general business model, emphasising the free-to-play model. This demonstration illustrates the interrelations between this business model and the surveillance economic ecosystem. We then focus on the persuasive design strategies implemented by mobile games to ensure recurring and prolonged player connection, thus highlighting the various deceptions that some companies use to exploit individuals' gaming activity and prevent them from fully understanding consent issues raised by gaming apps. We then examine these issues in the context of the North American and European regulatory frameworks, underlining the shortcomings of the legal protection that citizens – particularly children – are given. Subsequently, we examine these legal flaws in relation to the current social context, which promotes individuals' transparency and considers data collection as standard, to the point of being unproblematic, invisible, and indisputable. Finally, the Foucauldian notion of dispositif is used to analyse how mobile gaming is perceived as an assemblage of several elements, thus allowing us to explain the disciplinarisation of players to participate directly and voluntarily in this ludocapitalist surveillance dispositif.

Mobile game business models – from free-to-play to pay-to-win

Beginning in the early 2000s, data collection on player behaviour by videogame companies slowly gained popularity as technological developments advanced: network gaming, digital distribution, mobile games, and online console gaming. This widespread data collection practice resulted in a shift toward a data-driven industry (Whitson, 2013). Among its various iterations, three major business models are now prevalent: premium games, downloadable content, and games as a service (Nieborg, 2016b).

The premium games model refers to the conventional concept in which players must purchase a videogame to enjoy it (Nieborg, 2016b). In contrast, the downloadable content model focuses on additional content, either in the form of a game expansion or cosmetics goods that players can purchase for a lesser fee (Lee et al., 2015). Lastly, the games-as-a-service model provides access to videogame titles through a monthly or annual subscription, much like the paradigm shift operated by several large software developers. Along these various models, developers use player data to modulate the in-game experience and assist in their design choices, such as incorporating features that promote extended connection times. However, the business model that relies most heavily on monetising players' data is the free-to-play model (Nieborg, 2016a).

In addition to encouraging the videogame industry to reconsider its economic strategies, technological advancements such as smartphones and tablets have contributed to the rising popularity of gaming. Supported by their high global adoption rates, mobile devices have swiftly imposed themselves as the platform of choice for many gamers and developers (Newzoo, 2021). In the Nordics, mobile phones are the preferred gaming platform (26%), outpacing consoles (11%) and personal computers (21%) (Deloitte, 2019). The revenues generated by this segment attest to its new popularity; in 2020, the mobile gaming market accounted for 52 per cent of the industry's overall revenue, totalling USD 79 billion (Newzoo, 2021). However, unlike console or computer games, mobile games are frequently available for free, thus leading the industry to explore alternative forms of income compatible with this medium and consumers' expectations.

Based on preexisting models, the videogame industry established various monetisation sources over the years. While sporting different names, the mobile games business models rely primarily on two sources of income: microtransactions and ad revenues (Whitson, 2019). Microtransactions, ubiquitous in free-to-play (also called freemium) mobile games, usually take the form of consumable (one-time-use) or non-consumable (permanent-access) items, granting players game advantages, whether functional or aesthetic (Alha, 2020). These virtual items, which range in price from a couple to over a hundred US dollars, provide studios with a simple income stream. This business model uses the collection of personal data to predict player behaviour by creating consumer profiles to present offers on items at times when the probability of purchase is highest (Nieborg, 2016a). The exploitation of these possible purchase behaviours even gives rise to what the industry has called whales (Balakrishnan & Griffiths, 2018). Central to the mobile game economic ecosystem, whales are the dedicated high-spending gamers who account for 2–5 per cent of the player population and whose purchases account for a significant portion of the mobile gaming industry's income (Whitson, 2019).

On the other hand, advertising sales are a substantial and consistent source of revenue for mobile games (Alha, 2020). More than selling spaces in the form of interstitial advertising, interactive commercials, native ads, or rewarded video ads, developers give advertisement companies access to their players' personal information. Under the guise of offering personalised advertising, these various commercial entities have access to data related to the mobile device used, including persistent information, such as device ID, serial number, SIM ID, but also personal and sensitive information like name, gender, address, postal code, e-mail address, location data, search terms, and medical information (Christl & Spiekermann, 2016; Reyes et al., 2018; Wijesekera et al., 2017).

Given the primarily opaque nature of the industry's data processing ecosystem, it proves challenging to piece together an accurate image (Nieborg, 2016a). Nonetheless, we can partially reconstruct this circuit by relying on players' acquisition process of mobile games combined with investigative work with field actors. The data collection process begins whenever a user accepts the terms of service of a mobile game, thus granting developers access to their personal information (Wijesekera et al., 2017). Specific data, such as device information, network connection information, or player activity, are initially collected and used to ensure the game's proper functioning (Reyes et al., 2018). Furthermore, mobile games encourage users to disclose additional personal information by sometimes requiring excessive permissions or allowing players to connect with their social network accounts (Alha, 2020; Kröger et al., 2021). Presented as a means of interacting with friends or preserving one's progress, the use of Facebook or Google accounts allows developers to connect the player's profile to their offline identity (Brückner et al., 2017; Christl, 2017).

Beyond the developers' use, the players' information is subsequently shared with advertising companies responsible for monetising the application. Through programmatic advertising techniques, ad providers then use this information to associate each player with offers relevant to them (Christl & Spiekermann, 2016). This complex procedure, also known as real-time bidding, refers to an automatic auction process involving multiple ad publishers bidding for advertising space related to specific consumer segments (Christl &

Spiekermann, 2016). Accordingly, this monetisation strategy includes many intermediaries with whom personal information might be shared. If developers declare in their privacy policies that the information collected is solely utilised for game stability and general operation, third parties with whom they conduct business, such as Google AdMob, AppsFlyer, or Mopub, are exempt from these conditions (Appfigures, 2022; Valentino-DeVries et al., 2018).

Accordingly, a vast quantity of data is acquired throughout players' mobile devices, including geolocation data and MAC address (Unity, 2020):

> By design, any third-party service bundled in an Android app inherits access to all permission-protected resources that the user grants to the app. In other words, if an app can access the user's location, then all third-party services embedded in that app can as well. (Reardon et al., 2019: 1)

These third parties, usually constituted of software development kits, provide developers with services assisting them in the various stages of their product's deployment, such as game engines, coding, analytical tools for crash reports, advertising, or financial services (Myrstad & Tjøstheim, 2021; Reardon et al., 2019). These development tools are commonplace, as a 2016 study calculated that free-to-play mobile game apps had an average of 18.6 third parties (Jonathan, 2016). While reducing the cost associated with development and game maintenance, these third parties lack transparency regarding their use of consumers' data. The ambiguity surrounding these critical security and ethical issues is even more concerning, given that third-party vendors are free to share the data obtained with their own third parties (Myrstad & Tjøstheim, 2021).

The various entities partaking in this ecosystem can sell the data they have gathered to data brokers. The United States Federal Trade Commission (FTC, 2012: para. 2) defines these entities as "companies that collect personal information about consumers from a variety of public and non-public sources and resell the information to other companies". Data brokers specialise in profiling and predicting consumers' behaviours using large databases fed by public and private data on individuals' consumption patterns (Rieke et al., 2016). These profiles are later sold to other entities working in the marketing or risk assessments sectors (Myrstad & Tjøstheim, 2021)

While the general public is familiar with some of the major companies in this industry, primarily because of the development of credit scores, companies such as Acxiom and Equifax also created various consumer scores ranging from Job Security Score, Charitable Donor Scores, and even Medication Adherence Score (Christl & Spiekermann, 2016). Acquiring data, including personal identifiers from mobile devices, social network profile information, credit card usage, and public records, these companies generate profiles capable of inferring our desires before they occur (Myrstad & Tjøstheim, 2021).

The influence of these companies becomes even more significant when we consider that these various actors buy and sell each other's data (Christl & Spiekermann, 2016). Accordingly, the current state of mobile gaming and its commercial ramification makes it nearly impossible for users to track the companies with whom their data is shared. In their report, *Out of Control: How Consumers are Exploited by the Online Advertising Industry*, Myrstad and Tjøstheim (2021: 11) argued: "The extent of tracking and complexity of the adtech industry is incomprehensible to consumers, meaning that individuals cannot make informed choices about how their personal data is collected, shared and used". Consequently, the massive commercial surveillance throughout the adtech industry is at odds with our fundamental rights and freedoms. From this perspective, the practice of the mobile game, although innocuous at first sight, raises essential ethical questions regarding the surveillance ludocapitalism established by this industry.

Persuasive design – playing or being played?

Surveillance ludocapitalism partially shares the same economic logic as platform capitalism, often labelled the "fourth economic revolution" (Srnicek, 2017). The European Commission projected in 2017 that the personal data processing industry would generate EUR 1 trillion in revenue by 2020, accounting for roughly 8 per cent of the European Union's GDP (gross domestic product) (Thirani & Gupta, 2017). The longer users interact with and remain on a digital platform, the more wealth they create for the platform's owners. Users are developers' resources, but they are also the client of the transformed product: They are the audience of increasingly targeted advertising. Therefore, user attention is one of the foundations of platform capitalism (Citton, 2014).

In a world of information overload, data collectors and marketing agencies compete for users' attention. In these "Great Platform Wars", big digital platforms such as Facebook and Google use various techniques to keep users connected and engaged for as long as possible. Srnicek (2017: 58) argued that "the more activities a firm has access to, the more data it can extract and the more value it can generate from those data, and therefore the more activities it can gain access to". Thus, platforms constantly create new ways to access parts of users' lives, such as unified logins and monopolistic game stores.

Within the context of platform capitalism, mobile games also use various design techniques to capture and maintain the attention of as many users as possible. Games have an advantage: They are fun and can conceal the data collection behind quick and straightforward game mechanics, such as time-limited rewards, interval resource collection, or daily quests. From this perspective, developers implement many features based on persuasive design with the fundamental intent of directly influencing behaviour. Thus, the principles of this design approach rely on classical and operant conditioning and behavioural psychology.

Reinforcement techniques are the basis of the persuasive designs implemented by mobile game studios to "train" behaviour. As part of our research project, we compiled a comprehensive list of persuasive design tactics that benefit surveillance ludocapitalism. Some of the more prevalent strategies used in free-to-play games are as follows: 1) setting number or time limits on actions (e.g., energy regeneration), forcing the player to wait between gaming sessions in order to continue their progression, which causes them to think about the game often and make time during the day to play; and 2) giving players rewards each time they connect to the game (with, e.g., a daily or time limit on the gift they can receive), which, based on positive reinforcement, ensures that most players join at least once a day, thus creating a habit through conditioning.

Conversely, some games use negative reinforcement techniques, for example, possession removal, which involves threatening to take away a player's asset if they do not perform a given action at the designated time. This way of conditioning behaviour is considered more efficient, as the fear of losing something is stronger than the promise of winning a gift (loss aversion).

Furthermore, mobile games often implement irregular rewards and gambling mechanics (e.g., loot box), making it difficult to predict when the game will reward the player. According to operant conditioning and contemporary cognitive science, irregular rewards are more addictive: "Random rewards motivate players to engage in an activity with persistent effort to obtain a desired item" (Legner et al., 2019). Some games create a compulsion loop by gradually increasing the difficulty of obtaining rewards, the worth of which is always random. The desire to earn rewards, combined with serotonin responses, promotes obsessive behaviour, especially when the collection of rare rewards is encouraged.

The integration of online multiplayer mode also extends players' connection times by adding cooperative or competitive features:

> The fact that people respond socially to computer products has significant implications for persuasion. It opens the door for computers to apply a host of persuasion dynamics that are collectively described as social influence – the type of influence that arises from social situations. (Fogg, 2002: 90)

Following this idea, persuasive design uses known social dynamics such as peer pressure, social comparison, and fear of missing out to influence users' behaviours. Regarding the production and collection of personal data, persuasive design increases the return rate of players and time spent in a game to ensure a consistent output of data and advertising time.

Considering the capital invested and the market's competitiveness, some developers even employ design dark patterns explicitly aimed to deceive people into performing actions they do not necessarily intend to do (Hodent, 2020). For example, "platforms use [design tactics] to manipulate users into disclosing information" (Waldman, 2020: 105). While they are widespread in online platforms, these tactics are also present in videogames: "A gaming dark pattern is something that is deliberately added to a game to cause an unwanted negative experience for the player with a positive outcome for the game developer" (Dark Pattern Games, n.d). The website *Dark Pattern Games* (www.darkpattern.games) identifies many temporal, monetary, social, and psychological dark patterns.

These various design choices highlight the pervasiveness and apparent invisibility from which free-to-play mobile games can manipulate and mislead players' practices. Through design based on behavioural psychology, users are encouraged to extend their gaming sessions, link their social media accounts, and, in the process, share additional information about their whereabouts, habits, risk aversions, or their ability to delay gratification. This data obtained continuously over time could then be used to fine-tune companies' consumer profiles, resulting in more accurate predictions. Given the increasing sophistication of these techniques, it seems difficult, if not impossible, for individuals to avoid or protect themselves against these manipulations.

Deception and dishonesty – agreeing to terms of service

Concerns over consumer data usage have received considerable attention in recent years. The publications of various stories in mainstream media on the safety issues surrounding our online habits, added to the rising popularity of password managers and virtual private networks, may indicate that individuals have acquired greater digital literacy regarding cybersecurity (Ghosh, 2020; Ringel, 2021; Stahl, 2021; Wamsley, 2020; Winder, 2019). Despite increased awareness, individuals still find it challenging to discern how companies use their information. Terms of service agreements rarely provide information about which third parties have access to a player's data, and when they do, it is the consumer's responsibility to review those third parties' privacy policies (Myrstad & Tjøstheim, 2021).

These documents' lack of transparency extends beyond their substance and into their structure and verbiage. In their conference proceedings, "On The Ridiculousness of Notice and Consent: Contradictions in App Privacy Policies", Okoyomon and colleagues (2019) argued that mobile-app privacy policies employ ambiguous wording, an inadequate reading level of expression, and long-winded formats, which contributes to their vagueness. Furthermore, the design used by companies to communicate their privacy policies, while adhering to legal standards, is not suited for consumer comprehension. Ari Ezra Waldman (2018: 133) claimed in his article, "Privacy, Notice, and Design", that the current format of privacy policies represents "'unpleasant design,' or design that deters certain behaviours by exercising a form of social control against actors". Accordingly, these decisions, whether voluntary or not, made by service providers discourage individuals from informing themselves about the use of their personal information, thus preventing them from granting free and informed consent (Okoyomon et al., 2019).

Companies' deceptive practices are not limited to "manipulative and unfair" policies but also to their implementation (Waldman, 2018: 81–82). For instance, numerous applications for children include contradicting information about safety measures implemented to safeguard minors. Analysing 8,030 apps published under the Google Play Store's "Designed For Families" section, Okoyomon and colleagues (2019: 5) discovered that 9.1 per cent of them (728 apps) expressed in their privacy policies that their products are not aimed at children under 13 years old, thus indicating inconsistency between the nature of their products and their legal records. Furthermore, 30.6 per cent (2,457 apps) of the apps studied maintained that they are "not knowingly" collecting personally identifiable information from minors under the age of 13 (Okoyomon et al., 2019: 5). As Okoyomon and colleagues pointed out, this is even more problematic, as it implies that developers are oblivious about the data they collect and share with third parties.

If companies cannot protect the personal data of the most vulnerable population, adult data privacy violations are also prevalent, enabling surveillance capitalism via mobile gaming. Accordingly, privacy policies' lack of transparency, confusing terminology, and developers' non-compliance underline the need to protect individuals and regulate the industries benefiting from data collection.

Legal and regulatory framework – playing between the lines

There is currently little legislation governing the collection and use of players' data by videogame developers. Examining the current laws in North America, Europe, and the Nordic countries reveals that individuals are sometimes poorly or insufficiently protected and that these regulations do not reflect the current technological context.

Information collection is regulated in Canada by the Personal Information Protection and Electronic Documents Act (PIPEDA). This Act, intended to safeguard Canadians whose personal information is collected by commercial entities, does not include any provisions relating to minors (PIPEDA, 2019). Accordingly, from a legal standpoint, no distinction is made between adults, adolescents, and children, leaving Canadians unprotected. Furthermore, this federal legislation has been criticised for being ill-suited to the current digital environment, its limited actions in assigning sanctions, and its difficulty in holding companies accountable for personal data breaches (Terrien, 2021).

The US has no federal regulations dedicated explicitly to protecting its citizens' data against commercial use (Rieke et al., 2016). In their report, *Data Brokers in an Open Society*, Rieke, Yu, Robinson, and von Hoboken

(2016: 16) described the American legal landscape as “a patchwork of sector-specific laws [that] govern the collection and use of personal information in certain situations, in certain sectors, or by certain types of entities”. Thus, the laws implemented provide limited and circumstantial safeguards. These legislations aim to ensure the confidentiality of medical data by healthcare providers and insurers (Health Insurance Portability and Accountability Act), the protection of data used by credit companies (Fair Credit Reporting Act), and the protection of communications exchanged by verbal or electronic means (Electronic Communications Privacy Act) (Rieke et al., 2014).

Although no federal law specifically addresses the data collected in the context such as mobile gaming, minors are covered by the Children’s Online Privacy Protection Act (COPPA). COPPA, which was approved in 1998, adopted in 2000, and updated in 2013, requires service providers who collect personal information from children under the age of 13 to make their privacy policies, which outline how personal data is gathered and handled, widely available to the public (FTC, 2020). Parents must also be directly informed about data collection and privacy policies, and their consent must be obtained before children access their products. Finally, users must have the opportunity to withdraw their consent and delete the data collected. While COPPA defines civil penalties for non-compliant operators, the Federal Trade Commission has sanctioned only eight service providers in the last three years (PRIVO, n.d.). However, Reyes and colleagues (2018) described these cases as “isolated incidents” in their article, “Won’t Somebody think of the Children? Examining COPPA Compliance at Scale”.

In Europe, the General Data Protection Regulation (GDPR) is undoubtedly the law that best protects individuals, although it could be stricter (GDPR, 2018). Adopted in April 2016 and implemented in May 2018, the GDPR aims to protect the privacy of European Union residents while also harmonising the numerous regulatory measures of its nations (Rieke et al., 2016). This legislation focuses on personal data processing, safeguarding one’s fundamental rights and freedoms relating to information privacy, and holding the entities involved in the data processing accountable for their actions.

The GDPR acknowledges the importance of protecting children’s data, and according to article 8, it is legal to collect and handle data from minors above 16 (GDPR.EU, 2018). However, service providers can lawfully use the data of minors aged 16 and under with the consent of the child’s parent or guardian. This article also stipulates that companies must exercise reasonable effort to obtain and verify parental consent. It is worth mentioning that GDPR’s members can lower the age of consent to 13 years old, which Denmark, Finland, Norway, and Sweden implemented (Macenaite & Kosta, 2017). The exclusion of this demographic group from digital platforms was a significant point of contention during the law’s passage, with many supporters believing that it would be detrimental to children's freedom of expression and right to information (Macenaite & Kosta, 2017).

In addition to being protected by the European Union legislation, the Nordic countries have adopted additional regulations to address some of the GDPR's shortcomings. These laws, which complement the GDPR and thereby better safeguard Nordic citizens, do not provide further protection for minors. As a result, children aged 13 and up are legally regarded as adults in Denmark, Finland, Norway, and Sweden regarding data processing (Macenaite & Kosta, 2017).

In the event of non-compliance with these regulations, the GDPR can enforce administrative fines based on the severity of the offence (GDPR, 2018). Accordingly, the penalties attributed are based on a series of criteria, such as the nature, severity, duration, harm done to consumers, and the company's intentional or negligent conduct. Since its implementation in May 2018, the GDPR imposed 940 fines for a total sum of EUR 1,556,179,408 (CMS, 2022). Although the GDPR constitutes one of the most robust legislations to date, several challenges related to its enforcement remain. Among these are the countries' disparities in interpretation, application, and fines assessment procedure regarding the offenders' financial operations (Rieke et al., 2016; McKean et al., 2022).

Aside from these numerous laws, the videogame industry has tried to self-regulate its activities and assist consumers in making more informed decisions. Examples include videogame rating systems such as the Entertainment Software Rating Board (ESRB) and Pan European Game Information (PEGI). Although this grading system is entirely voluntary, some businesses insist on its inclusion in the items they sell. In this sense, access to specific sales platforms represents one of the only incentives for developers to use these tools. However, these self-regulation programmes solely evaluate the game's content (ESRB, n.d.; PEGI, n.d.). While shown alongside the game classification, interactive or content elements such as in-game purchases or user interactions do not affect a product's rating (ESRB, n.d.). Digital games, like mobile games, can also obtain a rating under the International Age Rating Coalition (IARC), enabling digital sales platforms to display the appropriate rating according to the organisation's guidelines in place in the user's country (IARC, n.d.). None of the above are reliable indicators of player privacy protection or compliance with legislation such as COPPA or the GDPR (Falzon, 2019; PEGI, n.d.).

On the other hand, some self-regulatory programmes explicitly target data collection from kids under the age of 13. This voluntary initiative, known as the Safe Harbor Program, is implemented by COPPA, and the US Federal Trade Commission allows developers to obtain certification from an approved association indicating that their products are COPPA-compliant. However, this programme implemented to encourage the development of best practices is rarely used. As the research by Reyes and colleagues (2018) reveals, it is difficult to identify companies that have obtained the Safe Harbor certification, even on the accrediting bodies' websites. Furthermore, the authors point out in their research that the practices of Safe Harbor accredited apps are neither more secure nor COPPA-compliant. Indeed, Reyes and colleagues discovered that some of these programmes communicate players' permanent IDs through insecure networks and employ third parties whose usage is specifically prohibited in goods aimed at minors (Reyes et al., 2018). Therefore, it is apparent that the self-regulatory instruments and their enforcement by the legislative body are merely accessories and contribute very little to protecting children's data.

Although the United Nations Human Rights Office recognises digital privacy as a human right, and numerous nations have enacted legislation to that effect, individuals are still inadequately protected (Human Rights Watch, 2018; OHCHR, 2019). Accordingly, the present regulations are unsuited to the economic ecosystem that has evolved around the data processing sector. While the American legislation focuses more on the permitted commercial uses of personal data, the European GDPR provides thorough guidelines and sanctions to protect its citizens' digital privacy. The legislation shortcomings become even more apparent when considering the globalised nature of mobile games. Accordingly, regulatory agencies may find it challenging to implement sanctions on non-compliant entities due to the blurring of boundaries between developers' countries of origin, the geographical location of their data servers, and the user's location. Whether in North America or Europe, the current legislative landscape is far from sufficient to ensure citizens' digital privacy, especially for minors. This is particularly alarming as the data and predictive analytics industry has experienced significant growth in recent years.

Social discourses, surveillance, and mobile games – "I have nothing to hide"

Despite the privacy concerns about the mobile gaming industry, few voices have been raised against this surveillance ludocapitalism system. The omnipresence of digital technologies in the contemporary Western world makes these economic models acceptable due to the invisibility of these technical devices. For example, mobile phone penetration rates in Europe are 70 per cent, but in the Nordic countries, the rate rises to 92 per cent on average (Statistica, 2021), demonstrating the technology's pervasiveness in this region. The concept of habituation is helpful in understanding how technological devices slowly become invisible as they spread and become entangled with everyday life. Fickers and van der Oever (2020: 71) defined habituation as the "dissipitation of a target-psychological response, e.g. psychophysiological activation at the presentation of a novel stimulus due to repeated exposure only". Over time, what shocks or seems strange at first sight gradually ceases to have this effect and becomes a regular part of life without needing much attention. The habituation of users makes these digital technologies invisible, familiar, and standardised.

Habituation coupled with the acceleration of technological innovations, societal changes, and the ever-accelerating rhythm of life (Rosa, 2010) facilitates rapid ways of thinking. Rosa (2010) demonstrated, through his "social critique of time", that the frantic pace of our lives encourages us to crave smaller but more short-term and guaranteed gratifications: We believe that the growing practice of mobile gaming could be understood in this accelerated context of rewards and conditioned behaviour. Mobility enables this fluid and practically omnipresent activity, monetising every bit of "spare time" with regular tiny gratifications.

The collection of personal data is similar in many platforms and mobile games. As the relative importance of social media platforms such as Facebook, TikTok, and YouTube grow, surveillance becomes part of everyday life (Trottier, 2016). Therefore, when mobile games start to collect personal data and sell them to third parties, individuals will not necessarily pay attention to it (and the game's condition of use) – it already happens on every other platform, every day, and everywhere. This habituation, initially considered at the psychological level, thus becomes social when it becomes part of the discourse that trivialises and normalises the use of these technologies and traceability. The ubiquitous use of the Internet in our everyday lives has made data collection a seemingly unavoidable norm.

As we have shown elsewhere (Bonenfant et al., 2018, 2019; Crémier et al., 2019), current discourses regarding the production and circulation of data present it as a natural fact about computers and digital technologies rather than rational decisions. Geological metaphors such as "raw data", "data mining", "new gold", and so on, contribute to the social depiction of data as a natural resource waiting to be used (Gitelman, 2013; Puschmann & Burgess, 2014; van Dijck, 2014). As a socially depicted natural "resource" or "force", the economical use of personal data is easy to justify in a neoliberal society. Those with financial interests ensure minimal opposition, and citizens do not appear to have much authority to confront this operating method. These metaphors hide that data production is always intentional: Mobile game developers and third parties write specific lines of code to create data each time a condition is met (e.g., each click, each ad view, etc.). Therefore, discourses concerning personal data surveillance plays a crucial role in their social acceptability.

Moreover, some tech executives, such as Google's former CEO, Eric Schmidt, value citizens' transparency by equating honesty with disclosing the totality of one's private life (Jennings, 2009). In their book *Transparent Lives*, Bennett and colleagues (2014) pointed out, among other trends, a "security culture", a "growing ambiguity of personal information", and a "global surveillance market". The well-known phrase "nothing to hide" becomes a social injunction that benefits a minority of personal data operators who profit from the general public's incomprehension of genuine privacy issues posed by these technologies (Andrejevic, 2007).

While the common perception of data as a natural resource and its injunction on transparency are critical to social acceptance, free-to-play mobile games, for their part, allow for the development of surveillance structures. Indeed, the ludic nature of mobile apps is often used to justify dubious ethical practices, such as collecting data not directly related to the game (e.g., GPS localisation without a specific game mechanic). Data collection looks innocuous when it is "just for fun" or "to maximise in-game pleasure", but game developers – and more importantly, their third parties – regularly neglect to disclose that the data's primary purpose is to be sold. Thus, mobile games' social discourse legitimises data collection and promotes the widespread acceptance of surveillance capitalism. The Foucauldian approach to power, discourse, and dispositif can help us better understand this socioeconomic system's conditions and possibilities.

A Foucaldian approach – "Here is my data, help yourself"

Michel Foucault's work centres on a critical examination of contemporary forms of power. Moving away from the substantialist approach, Foucault (1978) argued that power is understood as inequality within the various relationships we engage in throughout our daily life, creating a dominant and a dominated group. Accordingly, power is exercised on the individual level and not just by society's various institutions; thus, power has no defined subject, is dispersed, and can be challenging to identify. According to Foucault (1976), these inequities are enabled through the various discourses formulated by individuals belonging to the dominant status: Discourse acts as a device and a space within which power relations can be confronted.

Accordingly, the dominant group's discourse aims to reproduce and perpetuate the power structure in place using a variety of elements such as "gestures, attitudes, ways of being, behavioural patterns or spatial configurations" (Foucault, 1976: 123). Thus, discourses allow dominant groups to assert their position through multiple ways of being and doing that are not limited to language. However, one should not confuse discourse as the source of power relations; it rather constitutes a mechanism that allows them to be actualised. For example, personal data operators trivialise ludocapitalist surveillance by using specific expressions or overemphasising its transparency, consequently ensuring their position of power over the ordinary citizens who play free-to-play mobile games that they consider "inoffensive".

If discourse and power are inextricably linked, Foucault will then argue that these elements are actualised within what he calls a dispositif. He defines this concept as,

> a resolutely heterogeneous whole including speeches, institutions, architectural arrangements, regulatory decisions, laws, administrative measures, scientific statements, philosophical and moral philanthropic proposals; in short, what is said as well as what is not said. [...] Therefore, the *dispositif* is always inscribed in a game of power, but always linked to one or several limits of knowledge that emerge from it, but, just as much, condition it [translated]. (Foucault, 1977: 299)

Accordingly, Foucault understands the dispositif as the meeting of multiple components whose objective is to monitor and control individuals inscribed in specific power relations. As a result, the dispositif corresponds to the intersection of living and non-living, and said and unsaid, elements, having an incidence on the orientation of the forces at work (Lafleur, 2015). This concept can be understood as a network of elements allowing the power relationship to be exercised.

Surveillance occurring under ludocapitalism is made possible by a dispositif comprising the following elements: the current economic system, mobile and trackable technologies, mobile games' persuasive designs, a legislative and self-regulatory framework, our habit of using and carrying mobile phones, social discourse trivialising data collection, our ever-increasing pace of life, and so on. This ludocapitalist surveillance dispositif asserts and reiterates the dominant group's position over the dominated, thus impeding their privacy and freedom of thought and action.

Insofar as the dominant groups control the dominated's possible field of action, they benefit from leaving little room for potential resistance against the power structure in place. Hence, the numerous dispositifs of our daily lives can be transformed into disciplinary devices. Raffnsøe (2008) subsequently characterised discipline as a dressing tool preventing behaviours before they occur, thus interfering with individuals' everyday activities. It is crucial to emphasise that discipline does not create "ideal-type" subjects; instead, it encourages behaviours driven by the need to accomplish specific actions, dictated by the power relationships governing our everyday lives (Foucault, 1980).

In this sense, the dispositif plays a crucial role in disciplining bodies by indicating the encouraged and proscribed behaviours without coercion or physical force. Free-to-play mobile gaming is an excellent illustration of individuals' willingness to frequently engage with and carry tracking devices at all times, even if it means returning home if they forget them. Raffnsøe and colleagues (2014) further described this disciplinarisation in their article, "What is a dispositive? Foucault's historical mappings of the networks of social reality", as follows:

> It is an arrangement that makes certain social tendencies or inclinations more likely to occur than others. A given dispositive is itself brought about through several social actions and incidents and is constantly evolving and being displaced. A dispositive articulates a new level of normativity that has evolved through our way of interacting, while simultaneously effecting this interaction. (Raffnsøe et al., 2014: 4)

Ultimately, a dispositif is about disciplining behaviour and social relationships to the point of social control (Deleuze, 1990).

From this perspective, discipline defines the rules of conduct that ensure order and the maintenance of the power relationship by preventing dissenting behaviours. In this ludocapitalist surveillance dispositif, the subjects of the surveillance are not even aware of being watched anymore. More precisely, they have internalised the surveillance system to the point of participating in this contemporary panopticism: Those observed abide by the rules without knowing whether or not the supervisor is there (Foucault, 1975). Citizens discipline themselves by performing certain acts that reproduce and bring about the surveillance dispositif: They participate and are themselves part of the surveillance system that benefits an economic and political minority (Lyon, 2001, 2006).

We believe that the surveillance dispositif is even more pernicious in mobile gaming since individuals are "typically entertained", paralysing any opposition to this ludocapitalistic mode of exploitation. By employing persuasive design techniques and deceiving players about their terms of service, free-to-play mobile games increase the effectiveness of their data collection process. Encouraged by incentives and other behavioural conditioning techniques, players discipline themselves and reproduce large-scale surveillance until it becomes socially accepted.

Conclusion

This chapter aimed to provide a comprehensive overview of the interdependence between the mobile game ecosystem and everyday surveillance – and its widespread acceptance by citizens. To define this phenomenon, we have proposed the concept of ludocapitalist surveillance dispositif, based on the notions of ludocapitalism, surveillance capitalism, and dispositif. While some have raised security and ethical concerns associated with surveillance and videogames, our concept represents an effort to distinguish the surveillance occurring within free-to-play mobile games (Kröger et al., 2021; Myrstad & Tjøstheim, 2021; Reyes et al., 2018). We have demonstrated how players' everyday behaviours reproduce the surveillance ludocapitalist dispositif through the economic, technical, psychological, semiotic, legal, and social dimensions of mobile gaming. Accordingly, what appears to be a commonplace practice is embedded in an economic model based on the commodification of personal data and the distribution of targeted advertising. We have emphasised how persuasive design strategies further reinforce this economic model through mobile games developed to condition players to stay connected as much as possible, even if it makes them addicted. Despite its legitimacy, the industry-regulated framework is frequently misleading and difficult for citizens to understand. Laws are piecemeal, even those for protecting children, and inadequate concerning technological and economic transformations.

We have argued that collective habituation leads to a normalisation of mobile technologies and traceability, to the point of trivialising surveillance. Commercial data collection discourse that values citizen transparency neutralises any contestation or adoption of alternative technologies. Finally, we have postulated that the present context of social acceleration, frequent gratification, and the promotion of playfulness associated with connotations of innocuity also contribute to its normalisation.

The contributions of this research rest on the comprehensive portrait we have presented of the various actors involved in free-to-play mobile game surveillance. This particularity is even more critical considering the complexity and opacity surrounding the forces involved in this ecosystem. Furthermore, we contend that combining concepts unique to game studies and surveillance studies allowed us to go beyond the technical aspects of surveillance and analyse the predominant persuasive design strategies of free-to-play games.

From this perspective, we have defended the idea that mobile games contribute to this ludocapitalist surveillance dispositif by disciplining citizens as data producers and consumers of advertising – they enable this form of capitalism by diverting people's attention. From a semantic point of view, to divert is to turn away, deter, and distract, which is the act of distracting someone from their concerns. Similar to how many academics considered mass entertainment as ideological indoctrination (Horkheimer & Adorno, 1947; Marcuse, 1964), free-to-play mobile games has become a way to conceal large-scale data collection that benefits a minority at the expense of individuals' privacy. Used in this manner, playing seemingly harmless mobile games facilitates surveillance capitalism.

However, play as a practice has always had a socially beneficial role, as it is associated with freedom (Huizinga, 1938), creation (Fink, 1966), and the building of social relationships (Caillois, 1958). But in this ludocapitalist surveillance dispositif, mobile games become a means to discipline and control individuals. As we saw in the 2016 American elections (Jamieson, 2018), the risks of political manipulation are real: If targeted and personalised marketing can successfully sell products, it can equally sell ideas. The more precise advertising profiling becomes through massive data collection, the more influential political marketing campaigns will be, leaving individuals at risk of being directly manipulated by political groups. While the Nordic countries are among the world leaders in mobile game development, with companies such as King (Sweden), Supercell (Finland), and Rovio (Finland), it seems imperative that the actors of this industry question their practices and their implications in the erosion of our digital privacy. Consequently, all citizens are affected by these issues, whether they are gamers or not.

Acknowledgements

This research was conducted within the “Canada Research Chair on Big Data and Gaming Communities” and was funded by the Canadian Social Sciences and Humanities Research Council (SSHRC).

References

Alha, K. (2020). *The rise of free-to-play: How the revenue model changed games and playing* [Doctoral thesis, Tampere University]. http://urn.fi/URN:ISBN:978-952-03-1774-4

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. University Press of Kansas.

Appfigures. (2022). *Most popular SDKs in apps and games*. https://appfigures.com/top-sdks/all/all

Balakrishnan, J., & Griffiths, M. D. (2018). Loyalty towards online games, gaming addiction, and purchase intention towards online mobile in-game features. *Computers in Human Behavior*, *87*, 238–246. https://doi.org/10.1016/j.chb.2018.06.002

Bennett, C. J., Haggerty, K. D., Lyon, D., & Steeves, V. (Eds.). (2014). *Transparent lives: Surveillance in Canada*. Athabasca University Press. https://www.doi.org/10.15215/aupress/9781927356777.01

Bonenfant, M. (2021). Hypermodern video games as emblems of empire or how the gaming multitude adapts to hypermodernity. *Games and Culture*, *16*(3), 357–370. https://doi.org/10.1177/1555412020961849

Bonenfant, M., Crémier, L., & Lafrance St-Martin, L. I. (2018). Réflexions sémiotiques sur le circuit des données massives [Semiotic reflections on the big data circuit]. In A. Mondoux, & M. Ménard (Eds.), *Big data et société: Industrialisation des médiations symboliques* [*Big data and society: Industrialisation of symbolic mediations*]. Presses de l'Université du Québec.

Bonenfant, M., Lafrance St-Martin, L. I., & Crémier, L. (2019). Affected data: Understanding knowledge production in algorithmic events. *Global Media Journal*, *11(2)*, 66–78. https://www.proquest.com/scholarly-journals/affected-data-understanding-knowledge-production/docview/2434436008/se-2

Brückner, S., Sato, Y., Kurabayashi, S., & Waragai, I. (2017). The handling of personal information in mobile games. *International Conference on Advances in Computer Entertainment*, 415–429. https://doi.org/10.1007/978-3-319-76270-8_29

Caillois, R. (1958). *Les jeux et les hommes* [*Games and people*]. Gallimard.

Christl, W. (2017). *Corporate surveillance in everyday life: How companies collect, combine, analyze, trade, and use personal data on Billions*. Cracked Labs. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Christl, W., & Spiekermann, S. (2016). *Networks of control: A report on corporate surveillance, digital tracking, big data & privacy*. Facultas. https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf

Citton, Y. (2014). *L'économie de l'attention: Nouvel horizon du capitalisme?* [*The attention economy: New horizon of capitalism?].* La Découverte. https://doi.org/10.3917/dec.citto.2014.01

CMS. (2022). *GDPR Enforcement Tracker*. https://www.enforcementtracker.com

Crémier, L., Bonenfant, M., & L. I. Lafrance Saint-Martin (2019). Raw data or hypersymbols? Modelizing sign function in big data meaning-making processes, *Semiotica*, (230), 189–212. https://doi.org/10.1515/sem-2018-0110

Dark Pattern Games. (n.d.). *Helping you find healthy mobile games*. Retrieved January 28, 2022, from https://www.darkpattern.games/

Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle [Postscript on societies of control]. *L'autre Journal*, *1*.

Deloitte. (2019). *Smartphone: The center of life: A study on Nordic mobile consumer behaviour*. Deloitte Global Mobile Consumer. https://www2.deloitte.com/content/dam/Deloitte/se/Documents/technology-media-telecommunications/Global-Mobile-Consumer-Survey-2019-Nordic-Cut.pdf

Dibbell, J. (2007, June 17). The life of the Chinese gold farmer. *The New York Times*. https://www.nytimes.com/2007/06/17/magazine/17lootfarmers-t.html

ESRB. (n.d.). *Ratings guides, categories, content descriptors*. ESRB Ratings. Retrieved February 14, 2022, from https://www.esrb.org/ratings-guide/

Falzon, J. (2019, December 18). *Does an E or E10+ rating mean a game or app is "directed to children" for purposes of COPPA?* ESRB Ratings. https://www.esrb.org/privacy-certified-blog/does-an-e-or-e10-rating-mean-a-game-or-app-is-directed-to-children-for-purposes-of-coppa/

Fickers, A., & van der Oever, A. (2020). (De)habituation histories: How to re-sensitize media historians. In N. Hall, & J. Ellis (Eds.), *Hands on media history: A new methodology in the humanities and social sciences* (pp. 58–75). Routledge. https://doi.org/10.4324/9781351247412

Fink, E. (1966). *Le jeu comme symbole du monde* [*The game as a symbol of the world*] (H. Hildenbrand & A. Lindenberg, Trans.). Éditions de Minuit.

Fogg, B. J. (2002). Persuasive technology: Using computers to change what we think and do. *Ubiquity* (December), Article 5. https://doi.org/10.1145/764008.763957

Foucault, M. (1975). *Surveiller et punir* [Surveil and punish]. Gallimard.

Foucault, M. (1976). Le discours ne doit pas être pris comme... [Speech should not be taken as...]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et* écrits*: 1976–1979* [*Said and written: 1976–1979*] (pp. 123–124). Gallimard.

Foucault, M. (1977). Le jeu de Michel Foucault [The game of Michel Foucault]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et* écrits *III 1976-1979* [*Said and written: 1976–1979*] (pp. 298–329). Gallimard.

Foucault, M. (1978). Dialogue sur le pouvoir [Dialogue about power]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et* écrits*: 1976-1979* [*Said and written: 1976–1979*] (pp. 464–476). Gallimard.

Foucault, M. (1980). Table ronde du 20 mai 1978 [Round table of 20 May 1978]. In D. Defert, F. Ewald, & J. Lagrange (Eds.), *Dits et* Écrits *IV* [*Said and written: 1976–1979*]. Gallimard.

FTC. (2012, December 18). *FTC to study data broker industry's collection and use of consumer data*. Federal Trade Commission. https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data

FTC. (2020). *Complying with COPPA: Frequently asked questions*. Federal Trade Commission. https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

GDPR. (2018, November 14). *Art. 83 GDPR – General conditions for imposing administrative fines*. GDPR.Eu. https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/

GDPR.EU. (2018). *Art. 8: GDPR conditions applicable to child's consent in relation to information society services*. https://gdpr.eu/article-8-childs-consent/

Ghosh, D. (2020, July 17). Don't give up on your digital privacy yet. *Slate*. https://slate.com/technology/2020/07/data-privacy-surveillance-law-marketers.html

Gitelman, L. (2013). *Raw data is an oxymoron*. MIT Press. https://doi.org/10.7551/mitpress/9302.001.0001

Hodent, C. (2020). *The psychology of video games*. Routledge. https://doi.org/10.4324/9781003045670

Horkheimer, M., & Adorno, T. W. (1947). *Dialektik der Aufklärung* [*Dialectic of enlightenment*]. Querido Verlag.

Huizinga, J. (1938). *Homo Ludens: Essai sur la fonction sociale du jeu* [*Homo Ludens: An Essay on the Social Function of Play*]. Gallimard.

Human Rights Watch. (2018, April 19). Data privacy is a human right. *Human Rights Watch*. https://www.hrw.org/news/2018/04/19/data-privacy-human-right

IARC. (n.d.). *How the international age rating coalition works | IARC*. Retrieved February 14, 2022, from https://www.globalratings.com/how-iarc-works.aspx

Jamieson, K. H. (2018). *Cyberwar: How Russian hackers and trolls helped elect a president: What we don't, can't, and do know*. Oxford University Press.

Jennings, J. (2009, December 11). *Google CEO: If you want privacy, do you have something to hide?* Computerworld. https://www.computerworld.com/article/2468308/google-ceo--if-you-want-privacy--do-you-have-something-to-hide-.html

Jonathan. (2016, June 2). *Slimming down: Fighting SDK fatigue and bloat*. AdColony. https://www.adcolony.com/blog/2016/06/02/fighting-sdk-fatigue/

Jordan, W. G. (2014). *Ludocapital: The political economy of digital play* [UC Irvine]. https://escholarship.org/uc/item/0985k4rw

Kröger, J. L., Raschke, P., Campbell, J. P., & Ullrich, S. (2021, July 6). Surveilling the gamers: Privacy impacts of the video game industry. *SSRN*. https://doi.org/10.2139/ssrn.3881279

Lafleur, S. (2015). Foucault, la communication et les dispositifs [Foucault, communication and devices]. *Communication. Information Médias Théories Pratiques*, *33*(2). https://doi.org/10.4000/communication.5727

Lee, J. H., Jett, J., & Perti, A. (2015). The problem of "additional content" in video games. *Proceedings of the 15th ACM/IEEE-CS Joint Conference on Digital Libraries*, 237–240. https://doi.org/10.1145/2756406.2756949

Legner, L., Eghtebas, C., & Klinker, G. (2019). Persuasive mobile game mechanics for user retention. *Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 493–500. https://doi.org/10.1145/3341215.3356261

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. McGraw-Hill Education.

Lyon, D. (2006). *Theorizing surveillance: The panopticon and beyond*. William Publishing.

Macenaite, M., & Kosta, E. (2017). Consent for processing children's personal data in the EU: Following in US footsteps? *Information & Communications Technology Law*, *26*(2), 146–197. https://doi.org/10.1080/13600834.2017.1321096

Marcuse, H. (1964). *One-dimensional man*. Beacon Press.

McKean, R., Kuroska-Tober, E., & Waem, H. (2022). *GDPR fines and data breach survey: January 2022*. DLA Piper. https://www.dlapiper.com/en/austria/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/

Merton, R. K. (1948). The self-fulfilling prophecy. *The Antioch Review*, *8*(2), 193–210. https://doi.org/10.2307/4609267

Myrstad, F., & Tjøstheim, I. (2021). *Out of control: How consumers are exploited by the online advertising industry*. https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

Newzoo. (2021). *Newzoo global games market report*. https://newzoo.com/insights/trend-reports/newzoo-global-games-market-report-2021-free-version/

Nieborg, D. B. (2016a). Free-to-play games and app advertising: The rise of the player commodity. In J. F. Hamilton, R. Bodle, & E. Korin (Eds.), *Explorations in critical studies of advertising* (pp. 38–51). Routledge. https://doi.org/10.4324/9781315625768

Nieborg, D. B. (2016b). From premium to freemium: The political economy of the app. In T. Leaver, & M. Willson (Eds.), *Social, casual and mobile games: The changing gaming landscape* (pp. 225–240). https://doi.org/10.5040/9781501310591.ch-016

OHCHR. (2019). *OHCHR and privacy in the digital age*. UN High Commissioner for Human Rights. https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

Okoyomon, E., Samarin, N., Wijesekera, P., Elazari Bar On, A., Vallina-Rodriguez, N., Reyes, I., Feal, Á., & Egelman, S. (2019). On the ridiculousness of notice and consent: Contradictions in app privacy policies. *Workshop on Technology and Consumer Protection (ConPro 2019), in Conjunction with the 39th IEEE Symposium on Security and Privacy*. https://www.ieee-security.org/TC/SPW2019/ConPro/papers/okoyomon-conpro19.pdf

PEGI. (n.d.). *PEGI age ratings*. Retrieved February 14, 2022, from https://pegi.info/page/pegi-age-ratings

PIPEDA. (2019). *Testimony of PIPEDA*. https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

PRIVO. (n.d.). *History of COPPA violations*. Retrieved February 14, 2022, from http://www.privo.com/history-of-coppa-violations

Puschmann, C., & Burgess, J. (2014). Metaphors of big data. *International Journal of Communication*, *8*, 1690–1709. https://ijoc.org/index.php/ijoc/article/view/2169/1162

Raffnsøe, S. (2008). Qu'est-ce qu'un dispositif? L'analytique sociale de Michel Foucault [What is a dispositive? The social analytics of Michel Foucault]. *Symposium*, *12*(1), 44–66. https://doi.org/10.5840/symposium20081214

Raffnsøe, S., Gudmand-Høyer, M. T., & Thaning, M. S. (2014). *What is a dispositive? Foucault's historical mappings of the networks of social reality* [Working paper, Copenhagen Business School, Denmark]. https://hdl.handle.net/10398/9077

Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., & Egelman, S. (2019). 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. *28th USENIX Security Symposium (USENIX Security 19)*, 603–620. https://www.usenix.org/system/files/sec19-reardon.pdf

Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., & Egelman, S. (2018). "Won't somebody think of the children?" Examining COPPA compliance at scale. *Proceedings on Privacy Enhancing Technologies*, *2018*(3), 63–83. https://doi.org/10.1515/popets-2018-0021

Rieke, A., Yu, H., Robinson, D., & von Hoboken, J. (2014). *Data brokers: A look at the Canadian and American landscape*. https://www.priv.gc.ca/media/1778/db_201409_e.pdf

Rieke, A., Yu, H., Robinson, D., & von Hoboken, J. (2016). *Data brokers in an open society*. Open Society Foundations. https://www.opensocietyfoundations.org/publications/data-brokers-open-society

Ringel, G. (2021). *Council post: Rethinking privacy: The road to data ownership*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/08/02/rethinking-privacy-the-road-to-data-ownership/

Rosa, H. (Ed.). (2010). *High-speed society: Social acceleration, power, and modernity*. Penn State Press.

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Stahl, A. (2021). *What you need to know to protect your data online*. Forbes. https://www.forbes.com/sites/ashleystahl/2021/06/04/what-you-need-to-know-to-protect-your-data-online/

Statistica. (2021). *Mobile devices in the Nordics*. https://www.statista.com/study/38811/mobile-device-usage-in-the-nordics-statista-dossier/

Terrien, D. (2021, June 15). *L'avenir de la réforme des lois sur la protection des renseignements personnels au Canada* [*The future of privacy law reform in Canada*]. https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2021/sp-d_20210526/

Thirani, V., & Gupta, A. (2017). *The value of data*. World Economic Forum. https://www.weforum.org/agenda/2017/09/the-value-of-data/

Trottier, D. (2016). *Social media as surveillance: Rethinking visibility in a converging world*. Routledge. https://doi.org/10.4324/9781315609508

Unity. (2020). *Privacy policy hub*. https://unity3d.com/legal/privacy-policy

Valentino-DeVries, J., Singer, N., Keller, M. H., & Krolik, A. (2018, December 10). Your apps know where you were last night, and they're not keeping it secret. *The New York Times*. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Waldman, A. E. (2018). Privacy, notice, and design. *Stanford Technology Law Review*, *21*(1), 74–127.

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, *31*, 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025

Wamsley, L. (2020, October 13). *Your technology is tracking you: Take these steps for better online privacy*. NPR. https://www.npr.org/2020/10/09/922262686/your-technology-is-tracking-you-take-these-steps-for-better-online-privacy

Whitson, J. R. (2013). Gaming the quantified self. *Surveillance & Society*, *11*(1/2), 163–176. https://doi.org/10.24908/ss.v11i1/2.4454

Whitson, J. R. (2019). The new spirit of capitalism in the game industry. *Television & New Media*, *20*(8), 789–801. https://doi.org/10.1177/1527476419851086

Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., & Beznosov, K. (2017). The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. *2017 IEEE Symposium on Security and Privacy (SP)*, 1077–1093. https://doi.org/10.1109/SP.2017.51

Winder, D. (2019, December 31). Get yourself cybersecure for 2020. *The Guardian*. https://www.theguardian.com/technology/2019/dec/31/get-cybersecure-for-2020-cybersecurity-passwords-smartphone

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2018). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

CHAPTER 2

To be a face in the crowd

Surveillance, facial recognition, and a right to obscurity

SHAWN KAPLAN

DEPARTMENT OF PHILOSOPHY, ADELPHI UNIVERSITY, USA

ABSTRACT

This chapter examines how facial recognition technology reshapes the philosophical debate over the ethics of video surveillance. When video surveillance is augmented with facial recognition, the data collected is no longer anonymous, and the data can be aggregated to produce detailed psychological profiles. I argue that – as this non-anonymous data of people's mundane activities is collected – unjust risks of harm are imposed upon individuals. In addition, this technology can be used to catalogue all who publicly participate in political, religious, and socially stigmatised activities, and I argue that this would undermine central interests of liberal democracies. I examine the degree to which the interests of individuals and the societal interests of liberal democracies to maintain people's obscurity while in public coincide with privacy interests, as popularly understood, and conclude that there is a practical need to articulate a novel right to obscurity to protect the interests of liberal democratic societies.

KEYWORDS: surveillance, facial recognition, privacy, right to obscurity in public, anonymity

Kaplan, S. (2023). To be a face in the crowd: Surveillance, facial recognition, and a right to obscurity. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillanc*e (pp. 45–66). Nordicom, University of Gothenburg.
https://doi.org/10.48335/9789188855732-2

Introduction

The proliferation of video surveillance cameras is astounding. It was approximated that there would be over 1 billion surveillance cameras globally by 2022, with China accounting for over half and the US for 85 million (Lin & Purnell, 2019). Though many have voiced privacy concerns over ubiquitous video surveillance, opinion has been divided in the philosophical literature as to whether this practice violates a right to privacy. The reasons for the philosophical debate range from fundamental disagreements about the existence of a distinct right to privacy (Thomson, 1975), to more specific concerns about whether a right to privacy can be properly extended to what people do in public (Nissenbaum, 1998; Ryberg, 2007), or whether discreet video surveillance ever wrongs individuals who are unaware of being observed (Alfino et al., 2003), or whether the mining of personal information wrongs anyone if the information is not misused (Alfino et al., 2003; Ryberg, 2007). In this chapter, I explore how the emergence of highly effective facial recognition technology reshapes the debate over video surveillance.[1]

We are on the cusp of a radically altered surveillance landscape, as facial recognition programs are used to augment, for example, our extensive video surveillance infrastructure, body cameras worn by police, and video cameras deployed on drones. Until recently, real-time video surveillance required a human monitor to assess security risks. Quite often, however, video surveillance data has been used *post-factum* to investigate criminal cases or to redesign security procedures.

Two fundamental things change when video surveillance is augmented with facial recognition: 1) the data collected is no longer anonymous but is linked to specific individuals, and 2) the data can be powerfully aggregated to produce detailed profiles of individuals. In the first instance, as opposed to obtaining data via CCTV regarding crowd numbers, facial recognition surveillance (FRS) can catalogue every person who participates in public protests, political rallies, religious observances, or any socially stigmatised activity. These individuals will no longer be nameless faces in the crowd but will be clearly identified, and their participation will become part of their digital record. In the second instance, using our publicly observable movements, behaviours, preferences, and associations, FRS data can be aggregated and analysed to produce immensely detailed profiles that will disclose much of our intimate details –including psychological propensities. Though profiling is not novel to FRS, I argue that the breadth and depth of this form of surveillance profiling is novel in the degree of the harms it threatens to cause.

Both troubling practices are ongoing in China. In Chongqing, a program connects “the security cameras that already scan roads, shopping malls and transport hubs with private cameras on compounds and buildings, and integrate them into one nationwide surveillance and data-sharing platform” (Denyer, 2018: para. 6). By augmenting this integrated system of video surveillance with facial recognition, Chinese authorities hope to track the movements, beliefs, and associations of their citizens to generate aggregate profiles. The larger ambition of the Chinese government is to combine this surveillance data with criminal, credit, and medical records, as well as online activity, to derive a "social credit" score by which each citizen's "trustworthiness" will be ranked (Botsman, 2017; Denyer, 2018). It is also suspected that FRS was used to track and arrest dozens of dissidents, petitioners, and journalists prior to the 2016 G-20 summit meeting in Hangzhou (Denyer, 2018).

Police in London, South Wales, Detroit, and Orlando have been testing FRS (Burgess, 2018; Harmon, 2019; Kaste, 2018), and it has been credited for over 300 arrests in Dubai over one year (Al Shouk, 2019). In addition, a leading manufacturer of police body cameras has added facial recognition capabilities to their products (Harwell, 2018). While assurances are given in the US that this surveillance technology would only be used to locate wanted criminals or missing persons, few jurisdictions have laws limiting the usage of FRS. In contrast, the EU has attempted to regulate FRS through the GDPR (European Parliament, 2016) and the recently proposed guidelines for harmonising rules on artificial intelligence (European Commission, 2021). Regardless, law enforcement in both Sweden and Finland have been judged to use facial recognition tools that fail to protect individuals' data (Skelton, 2021; Yle News, 2021), and a Swedish school district was fined for using FRS to track student attendance (Swedish Data Protection Agency, 2019). In addition, EU regulations have been interpreted to allow a Danish football team to use FRS to identify low-level offenders entering their stadium (Overgaard, 2019) and for Swedish stores to track shoppers' movements (Roos & Källström, 2020).

Considering the ability to use FRS to generate detailed profiles of individuals and to catalogue every individual participating in protests, political rallies, religious observances, or any socially stigmatised activity, Jake Laperruque (2017) has advocated for legal restrictions on facial recognition technology to protect our "right to obscurity" – that is, to remain a nameless face in the crowd. Insofar as the aim is to obscure individuals' identities when engaged in mundane, religious, and political activities *while in public*, a right to obscurity might appear entirely distinct from a right to privacy, which is conventionally assumed to restrict access to our non-public activities and intimate information. Whether the concerns raised by these two uses of FRS amount to a violation of a right to privacy, or a violation of a right to obscurity, or fails to amount to a rights violation at all, depends both upon what values or interests are threatened by FRS and which theory of privacy one accepts.

In the next section, I detail the values and interests threatened by the widespread use of FRS. My initial task is to distinguish how obscurity, as a public mode of anonymity, is distinguished from privacy. My analysis shows that widespread FRS will eliminate our obscurity while in public and that this institutional practice will unjustly impose risks of harm upon both individual members of the public and society. I consider potential justifying purposes of FRS and show that the associated risks imposed upon individuals and society are either unnecessary or disproportionate to the proposed benefits unless FRS is effectively regulated to protect our anonymity while in public.

In the third section, I consider whether the interests under threat from widespread FRS are best conceived of as privacy interests or whether the value of preserving our obscurity in public is best articulated as being distinct from privacy. Answering this question does not alter the normative arguments from the second section, nor does it call into question the regulatory policies proposed there. I propose that the question has pragmatic political significance for how we can most effectively advocate for policies and laws that will protect those interests and values under threat by FRS. Answering this question is, however, complicated by the lack of anything in the literature approaching a consensus for how to understand privacy. Considering the conceptual disarray surrounding privacy, I identify when the interests under threat by FRS coincide with plausible conceptions of privacy, and I assess whether the controversies surrounding those conceptions of privacy prove problematic when advocating for FRS regulation. I argue that the interests under threat from amassing detailed, aggregate profiles of individuals coincide with some conventional theories of privacy. In contrast, I show that the interests in need of protection when considering the use of FRS to catalogue participants in protests, political rallies, religious observances, or any socially stigmatised activity fall beyond the typical domain of privacy protections. I conclude that this discontinuity indicates a practical need to articulate a novel right to obscurity, as opposed to further broadening our conception of privacy.

Anonymity and obscurity in public

In this section, I provide an account of anonymity as obscurity in public and the general value it may offer. I then use this account to describe the way FRS eliminates our obscurity in public and the potential harms this poses to both individuals and to liberal democracies more generally.

The general value of obscurity in public

If anonymity is lost when FRS is broadly deployed, the question remains what exactly this loss amounts to. What is anonymity and what inherent or instrumental value does it hold? To be an anonymous face in the crowd is to enjoy broad obscurity regarding one's identity. Obscurity in public is a mode of anonymity wherein publicly observable information about each person (e.g., location and behaviour) is dissociated from their identity.

The inability to link some information to an individual identity is what differentiates anonymity from privacy. According to Julie Ponesse (2014), our personal information may become part of the public sphere and no longer be private but, insofar as the identifying markers have been sufficiently removed from that information, it can be dissociated from our identity, preserving anonymity. To illustrate, consider a traveller who tells everyone he encounters abroad that he is John Smith from England. Given the commonality of the name, it is only an opaque identifier and is readily dissociated from any identity; he still enjoys significant anonymity. His name and nationality are known to those to whom he revealed them, but all other aspects of his identity remain anonymous because, for this specific population, his other personal information remains dissociated. In a mirror image, the traveller who reveals her personal views and reasons for traveling to a stranger remains anonymous to the stranger insofar as her name and other identifying information remains dissociated.

The individual who is perceived by others as a mere face in the crowd enjoys broad anonymity because nearly all their identifying information remains dissociated and, thus, concealed from others. Is there something inherently valuable about this anonymity or obscurity while in public? To anonymously glide through a crowd can be a liberating experience, especially when compared to moving through a closed community where everyone knows who you are and takes note of your activities. Though such anonymity can be recognised as valuable, it may not be a universal good, as prolonged periods of anonymous obscurity might lead to a sense of alienation. The positive value of anonymity in this context is instrumental insofar as it removes inhibitions that can diminish an individual's autonomy. The absence of obscurity in public can create psychological pressure to conform to social expectations. However, we have no reasonable expectation that others who know us will not observe our public activities. Thus, nobody can claim a right to be an anonymous face in the crowd at any time they crave such obscurity. If a right to obscurity exists, it would be a conditional right.

The value of obscurity in public vis-à-vis facial recognition surveillance

Using this analysis of anonymity, we can quickly recognise how FRS would eliminate much of the anonymity people currently enjoy while in public. All FRS data is associated with an individual's identity, and an FRS network makes countless observations of individuals' movements, modes of transport, social contacts, purchases, attitudes, tastes, and behavioural idiosyncrasies. Much of the content of these individual data points will be ethically innocuous, but they will *not* be anonymous. However, the ease in which this non-anonymous raw data can be aggregated and analysed makes individuals vulnerable to significant harms.

This concern conforms to a focus upon the "inferential fertility" of information (Manson et al., 2007), as opposed to the ethical relevance of the informational content. Adam Henschke (2017) has made an extended argument for why we must take due care with how seemingly innocuous personal information is collected, analysed, shared, and used. He describes that, as this seemingly innocuous personal information is aggregated and integrated, a virtual identity is created, and this is ethically significant insofar as a virtual identity shapes how institutions and other persons interpret that individual or group. Of course, our virtual identities are already being constructed, without the use of FRS, based upon our purchasing records and online activities. Our virtual identities are commodified and sold, typically to those interested in marketing products or finding an audience susceptible to a political message or misinformation. FRS data would be a powerful source for constructing virtual identities by compiling our movements, behaviours, interests, social contacts and associations, demonstrated beliefs, psychological propensities, as well as political and religious activities. The creation of such detailed profiles makes people vulnerable to a range of possible harms. Following Robert Goodin (1985), Henschke interprets vulnerability as being under a threat of some harm and asserts that, if we make others vulnerable to us, we have a special duty to protect them from these potential harms. According to Henschke (2017: 223), we have a special duty to take due care with the personal information gained via surveillance technologies and that due care requires that "surveillance technologies with a potential to construct Virtual Identities ought to be designed and used in such a way as to minimise the probability and magnitude of information harms".

I agree that, when our actions or policies make others vulnerable to harms, we have a special duty to minimise the probability and magnitude of those harms. However, this seems to be a moral concern secondary to the question of whether we have wronged individuals by imposing an unjust risk of harm upon them in the first place. (Risk of harm is here understood as the product of the probability of a harm and the magnitude of that harm.) To show how FRS imposes an unjust risk of harm, I describe the harms this form of surveillance makes us vulnerable to, and then I show these risks of harm to be unjustly imposed. To do so, I must show that one of the following three necessary conditions for justified risk imposition is not satisfied: 1) the action or policy creating a risk of harm must serve some justifying purpose; 2) the imposed risk of harm must also be *necessary* for accomplishing that purpose (i.e., if there is a way to attain the same justifying purpose without imposing, or imposing a lesser, risk of harm, then the risk is unnecessary and unjust); and 3) the imposed risk of harm must be proportionate to the benefit of the justifying purpose.

Much of the vulnerability for the subjects of FRS results from its ability to create nuanced and detailed psychological profiles of individuals. Some might contend that the creation of such detailed and *intimate* psychological profiles would directly harm individuals. To technologically pry into people's heads by aggregating and analysing their publicly displayed behaviour might easily feel like a violation of their privacy. In the next section, I return to this concern when considering popular conceptions of privacy and how they relate to FRS. For the present, I focus upon how the collection of this surveillance data makes people vulnerable to two types of harms and whether these risk impositions are just or unjust.

First, people become vulnerable to the harm of psychological manipulation as a result of these detailed psychological profiles. Similar concerns have been raised by the way that social media data is analysed to target specific psychologically susceptible individuals with false information (Rosenberg et al., 2018; Vélez, 2021). A significant distinction between the cases is that people have a choice to opt in or out of social media use. The practical ability of individuals to effectively mask their identity while in public every day is minimal. A second significant difference is the diversity of surveillance data available from FRS, where facial and bodily expressions provide a broader range of personal responses (e.g., anxiety, calmness, attraction, repulsion, pleasure, pain, interest, disinterest, depression, happiness, etc.) than online activity (e.g., search and click history, social media posts and reactions, and time spent hovering over online images, etc.). The vulnerability to psychological manipulation from FRS is not different in kind from what we already face, but it is different in degree. Online activity can reveal one's psychological propensities and inclinations but pales in regard to detail when compared to what would amount to countless hours of surveillance data from tracking our everyday activities while in public.[2] It is reasonable to suppose that, as the dataset grows and the tools of analysis become more nuanced, the resulting psychological profiles will allow for much more diverse, powerful, and coercive forms of psychological manipulation. Psychological manipulation which coercively triggers the target to adopt beliefs and actions is a violation of individual autonomy and a clear harm.

Second, detailed psychological profiles make individuals vulnerable to opportunity losses. Potential employers would no doubt pay handsomely to know the psychological propensities of job candidates, including their ability to focus or stay calm under pressure, their sociability, their lifestyle choices (e.g., substance use and abuse), their propensities for depression, anger, and violence, or their fit with management's religious and political views. If individuals' profiles indicate them to be statistically "riskier" hires, they could find many employment opportunities closed off. Parallel limits could be found when applying to schools and universities, or when seeking housing, insurance, and public assistance. Limiting a person's reasonable range of opportunities based upon what is publicly observable about them would stand as a harm insofar as a reasonable range of opportunities is required for living any conception of a good life. Even if opportunity loss does not rise to the level of denying individuals a reasonable range of opportunities, we can still acknowledge that the accumulation of micro-scaled opportunity losses can pose a morally serious harm.

It might be objected that, while the creation of detailed psychological profiles makes individuals vulnerable to harms from psychological manipulation and opportunity loss, that does not indicate an ethical problem with FRS but rather a concern about the misuse of the FRS data. Similar claims have been made regarding other surveillance and data-gathering technologies (Alfino & Mayes, 2003; Marmor, 2015). Ryberg (2007) argued that collecting data from non-augmented CCTV surveillance fails to wrong individuals if it is used for crime prevention. If the data were used differently, then we might very well have a reasonable moral complaint: "If CCTV administrators start working as some sort of private investigation company passing on or selling information to employers or other parties, then surely they are engaging in activities that go far beyond mere crime prevention" (Ryberg, 2007: 141). Nissenbaum (1998) describes this specific sort of misuse of data as a failure to respect the "contextual integrity" of the information by shifting it from a legitimate context (e.g., crime prevention) to another context without the subject's consent or providing justification.

No doubt, individuals can be harmed and wronged by such misuse of personal information gained by various forms of surveillance. However, this ignores the inferential fertility of the data being collected from FRS and how easily this data can be aggregated and analysed into profiles that put individuals at risk of serious harms. The mere collection of this non-anonymous data puts people at risk of psychological manipulation and opportunity loss. To echo Henschke (2017: 260), the degree of ease by which data can be aggregated into a virtual identity "tells us how far off it is from simple data". The collection of "simple data" might be morally neutral but, as data is more easily aggregated into a profile or virtual identity, this correlates with the growth of people's increased vulnerability to harms.

The objector might respond that we ought to simply respect the contextual integrity of the FRS data and not shift this data into the context of forming profiles or virtual identities. This response presupposes that there are justifying purposes for collecting FRS data. Perhaps it would be legitimate to use this technology to seek missing persons, track suspected criminals, or create profiles of suspected terrorists? Like other forms of targeted surveillance, FRS ought to require a court warrant and, if the courts are sufficiently rigorous, people will be less vulnerable. However, for facial recognition technology to effectively locate missing persons or carry out surveillance against suspected criminals, authorities cannot simply enter the face of the one person of interest. The accuracy of facial recognition machine learning is relative to the number and diversity of faces in the database. Even if FRS required a warrant to target specific individuals, it would only be reliably accurate if the majority of citizens had their facial biometrics entered into the database.

Furthermore, if this system of surveillance is meant to locate and track targeted individuals efficiently, then not only will our video surveillance infrastructure need to be universally augmented with facial recognition, but everyone would need to be tracked constantly. To hope that one person can be identified within tens of millions of video feeds (or more) would be like seeking a needle in a haystack. While super-computers can help speed the process of sorting through massive amounts of data to find a person of interest, it would be far more efficient to constantly keep track of everyone's movements. This is only to suggest that there would be pressure from the standpoint of efficiency to engage in non-targeted FRS and to access this data only in a targeted fashion after receiving a warrant. If this were to become standard practice, people would have unnecessary risks of harm imposed upon them, unless the data from this surveillance were anonymised in two important ways.

One significant protection would be to anonymise people's whereabouts by dissociating this data from their identity (i.e., dissociating location data from their names and identification numbers) until a warrant is granted. A further stage of anonymisation could be attained by banning any additional analysis of FRS data beyond location. This means blocking any analysis of observed behaviour and social connections. If location data were anonymised and dissociated from other personal information – like psychological propensities and social connections – then having the capacity to target individuals with FRS when ordered by a court would make people less vulnerable to serious harms from psychological manipulation or opportunity loss. Given the potential ability to subvert these anonymity protections, vulnerability would not be eliminated. The remaining risk imposed would still need to be proportionate to the likely benefits. Interestingly, these two protections would largely preserve individuals' anonymity in public, allowing them to remain mere faces in the crowd. Put differently, if we only find FRS permissible when anonymity is preserved in the two ways described, we have arrived at a conclusion that there are no *general* contexts in which non-anonymous data can be legitimately gathered via FRS.

It might be objected that building such anonymity protections within FRS systems might limit the potential to prevent predictable violence and criminal activity. For example, if the behavioural patterns preceding suicide attempts or terrorist attacks can be recognised via machine learning and effectively used to analyse real-time surveillance data, then banning the analysis of surveillance data beyond location would appear to significantly limit our capacity to prevent such violence. This, however, is only an apparent drawback. If our machine learning systems could predict likely violent or criminal activity by using surveillance data, it could do this both by learning from anonymous data and analysing anonymous real-time surveillance. If computers could analyse real-time surveillance better than human monitors for security risks, the resulting data could remain dissociated from any individual's identity. Once the automated system identifies a security risk, it could both alert a human monitor to look at the surveillance stream and have police dispatched to investigate. All of this could be done without linking observed behavioural patterns with individual identities. Thus, using such technology to help prevent violence and crimes does not mandate a loss of anonymity.

By dissociating location and behavioural data from specific identities, anonymity is preserved in a way that keeps personal information from being aggregated into psychological profiles. This, in turn, diminishes people's vulnerability to harms that FRS would otherwise create. Thus, real-time FRS which fails to serve these justifying purposes or imposes unnecessary risks of harm, by failing to anonymise the data and its analysis, would be an unjust imposition of risk. At the same time, if it is unlikely that governments will effectively protect people's anonymity by keeping the information gained from FRS dissociated from their identities, then it would be prudent from the standpoint of practical politics to ban states altogether from coupling video surveillance with facial recognition.

Thus far, I have considered the powerful capacity to form detailed profiles of individuals via FRS. I now focus on the second concern named at the start of this chapter: the ability to use FRS to catalogue individuals participating in protests, political rallies, religious observances, or any socially stigmatised activity. To join a large group to express dissent via protest or rally for common political cause, or to join in common religious belief and practices, obscures the participants' identities, as each appears as a mere face in the crowd. If participants fear repercussions as a result of being identified any time they engage in socially stigmatised activities or ones disapproved of by government authorities, then the increased negative social pressure will likely correspond to reduced individual autonomy.

This chilling effect of FRS is not equivalent to a *direct* violation of the rights to free expression, assemblage, or worship. Unlike cases where individual rights are directly violated (e.g., the mass arrest of protesters), cataloguing the identities of group members is an act of implicit intimidation where repercussions are made possible but are not explicitly threatened.[3] (However, if the same technology were used by the surveillance state to overtly intimidate its citizens, then this would easily rise to a violation of these civil rights.) This implicit intimidation undermines the *effective* ability of people to exercise their rights to free expression, assembly, and worship.

Given the vast power asymmetry between those carrying out surveillance and those who are the subject of this cataloguing, one could not easily blame the intimidated party for their psychological response. My point is not that this response is perfectly natural (though it may be). Instead, insofar as citizens are vulnerable to the state's asymmetric power which could deny their rights or impose negative repercussion for exercising their rights, the state and its law enforcements agencies have a special obligation towards those citizens. Beyond the responsibility of the state and its law enforcement authorities to avoid directly violating citizens' rights to free speech, assemblage, and worship, the state has a special obligation to create institutional practices that reassure citizens that they are not vulnerable to negative repercussions when they exercise these rights. Unless this special obligation is met, citizens will have their effective ability to exercise their rights undercut.[4]

When the effective ability to engage in free speech, assembly, and worship is diminished by the implicit intimidation from FRS, we must consider whether this inflicts a broader societal harm. When individuals feel so intimidated that they are reticent to either express dissent in peaceful protests or to assemble with others who share common political or religious beliefs, then the ability of a liberal democratic society to function well is diminished. For example, when the free expression of political dissent in protests or of political convictions at rallies is diminished, citizens will not be able to effectively challenge the political views of their compatriots, and democratic institutions will not be able to optimally represent the people's will because it remains partially silent. Also, when individuals are reticent to make their religious affiliations public, society appears more homogenous and is less capable of approximating the liberal ideal of supporting diverse ideas of the good. Without citizens being able to exercise these rights in a more optimal manner, broad societal interests of liberal democracies are undermined in significant ways, thus harming society.

By undermining the ability of liberal democracies to function well, the practice of cataloguing political or religious participants via FRS would be unjust, unless this societal harm were necessary and proportionate for attaining some justifying purpose. Perhaps FRS is permissible for cataloguing participants in riots or in group demonstrations of hate or bigotry? Regarding public demonstrations of hate or bigotry, our answer will hinge upon whether hate speech is protected under the right to free speech. If free speech rights protect hate speech, then cataloguing hate speech participants via FRS would unjustifiably undermine people's effective ability to exercise their right to free speech. If hate speech is *not* protected as free speech, then we can consider it in conjunction with the case of cataloguing rioters. These cases would involve employing facial recognition to identify criminals, and this can only be done *after* the crime has been committed. Since the aim is not crime prevention but a criminal investigation, *real-time* FRS is unnecessary. Instead, a warrant could be required to identify individuals engaged in criminal activities post factum. Thus, there are no obvious contexts for legitimately using real-time facial recognition to catalogue participants in any group activity. In the absence of a context where real-time cataloguing serves a legitimate justifying purpose, the harms imposed upon liberal democratic societies by such FRS would always be unjust.

In this section, I have developed an account of anonymity as obscurity in public and uncovered what is valuable about obscurity in public both for individuals and society. Though it may be liberating to be an anonymous face in the crowd, the incidental loss of one's obscurity in public does not constitute a significant harm. However, FRS would effectively eliminate all anonymity while in public. I have highlighted two worrisome contexts for the loss of one's obscurity while in public: the creation of detailed individual profiles based upon publicly observable behaviour and the cataloguing of individuals participating in protests, rallies, religious observances, or any socially stigmatised activity. I have argued that, in the first context, the mere collection of non-anonymous FRS data makes people vulnerable to harms due to the ease by which this data can be aggregated and analysed to create nuanced psychological profiles. By disclosing individuals' psychological propensities, they are made vulnerable to psychological manipulation and opportunity loss. Hence, anonymity as obscurity in public is linked to our individual interests in preserving our autonomy and maintaining a reasonable range of opportunities or, at minimum, avoiding regular micro-scaled losses of opportunities.

Though I acknowledged the ways FRS can positively serve societal interests in crime prevention and locating missing persons, I have argued that these apparently legitimate aims can be embraced while preserving much of our anonymity by setting the following limits: First, facial biometric data ought to be dissociated from individual identities until a court warrant is provided. Second, the gathering of this anonymous data ought to be limited to location. Any further behavioural analysis of FRS data ought to be banned unless that analysis is of anonymous data. Since the justifying purposes can be attained while imposing lesser risks of harm, I concluded that FRS, in the absence of the limits described, imposes unjust risks of harm.

In the second context, I have emphasised how preserving anonymity as obscurity in public serves the societal interest of liberal democracies to optimise citizen's free speech, free assembly, and free religious worship. While cataloguing participants in political or religious activities does not directly violate these rights, I have argued that the implicit intimidation of such surveillance tactics would undermine the effective ability of individuals to exercise their rights. Cataloguing individuals can only be justified for the sake of a legal or criminal investigation, and this does not require real-time FRS. Instead, a warrant could be required to identify criminal suspects post factum. Insofar as the real-time cataloguing of participants serves no legitimate purpose, this practice would impose unjust harms upon society.

I next consider whether these various interests fall under privacy interests or whether anonymity as obscurity in public is best kept distinct from privacy. Privacy advocates have long drawn a connection between privacy and individual autonomy; however, privacy is not typically associated with maintaining a reasonable range of opportunity, nor with the societal interest in supporting the effective ability of individuals to freely express dissent, assemble, and engage in worship. Does this discontinuity with conventional conceptions of privacy indicate a need to broaden our concept of privacy, or does it indicate that anonymity as obscurity in public is best kept distinct from privacy?

Obscurity, privacy, and rights

Judith Jarvis Thomson (1975: 295) famously stated, "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is". She argued that the cluster of rights that we associate with privacy can be reduced to other rights clusters, like property rights and rights over the person. Thomson's point was not that privacy is vacuous or unimportant, but that the concept has no independent explanatory power for *why* we have the rights in the privacy cluster. In opposition to Thomson, many privacy theorists have attempted to isolate what is fundamental and common to privacy claims and that makes privacy a distinct concept with explanatory power of its own. We remain far from anything like consensus or even broad agreement. As Daniel Solove (2008: 1) stated:

> Privacy, however, is a concept in disarray. Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.

If privacy does cover such a broad range of interests, then the search for a single defining characteristic of privacy might prove impossible. Is privacy the right to: be left alone (Warren & Brandeis, 1890), limit access to the self (Van Den Haag, 1971), keep secrets (Posner, 1981), control personal information (Fried, 1968), protect the integrity of personhood (Reiman, 1976), or protect an essential condition for intimacy (Rachels, 1975)? These defining characteristics of privacy proposed in the literature can each be criticised as being too broad, too narrow, too vague, or all three (Solove, 2008). This situation has led some recent privacy theorists (Henschke, 2017; Nissenbaum, 2010; Solove, 2008) to propose pluralistic accounts of privacy, where diverse conceptions are included under the umbrella concept of privacy. Though the pluralistic approaches are advantageous in capturing the wide uses of the term privacy, they struggle to explain the normative force of the concept or how the diverse conceptions of privacy properly limit one another when they potentially conflict with one another.

It is beyond the scope of this chapter to resolve the conceptual disarray surrounding privacy. Instead, I attempt to show when the interests in maintaining one's anonymity as obscurity in public readily coincide with some popular conceptions of privacy and which controversies are linked to those conceptions of privacy. I assess whether the controversies associated with the relevant conceptions of privacy create complications when advocating for protecting our obscurity in public. Where there is no direct overlap, I consider whether that obscurity interest in fact clashes with privacy conceptions or can be incorporated into a yet broader pluralistic conception of privacy.

Whether the limited claims to anonymity as obscurity in public outlined in the previous section coincide with a right to privacy or stand independently of privacy will not change the normative conclusions already drawn. At the same time, determining whether these obscurity interests coincide with already established conceptions of privacy, or require us to expand the umbrella concept of privacy, or stand independently from privacy claims, will make a difference at the level of policy and law. Resistance to the type of protections suggested in the previous section will likely come from those who find that protecting individuals' obscurity while in public exceeds what the right to privacy can reasonably protect. By mapping out the relationship between privacy and anonymity as obscurity in pubic, I hope to be able to remove resistance to establishing policy and law that will protect against the risks imposed by FRS. My goal is not to address all possible sources of political resistance to protecting our obscurity while in public, but those elements of resistance that are rooted in controversies surrounding how we conceive of privacy protections.

To start, aggregating and analysing FRS data into detailed psychological profiles violates a popular conception of privacy. While each individual data point may not coincide with what people typically think of as personal or intimate information, the resulting psychological profiles would very much fit such a description. The conception of privacy as control over personal information captures this concern. According to Charles Fried (1968: 482), "Privacy is not simply the absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves".

There are some immediate controversies related to this conception of privacy. First, if one were to consider control of personal information as *the* defining characteristic of privacy, then privacy rights would not protect us from physical or legal interference regarding what we do with our own bodies or how we raise our children. However, if we adopt a pluralistic concept of privacy, other conceptions which fall under the umbrella of privacy could address these other aspects. Second, this conception suffers from vagueness regarding what information is "personal" and what is meant by "control". If privacy were to mean complete control over all personal information, then this conception seems too broad. One reply is that privacy is control over "intimate" information (Inness, 2003), but this too suffers from vagueness. While we can debate where to draw the line between intimate and non-intimate information, some information lands clearly within the bounds of what is intimate, for example, what consenting adults do in their bedrooms and medical records (including the clinical notes of psychotherapists). If the profiles resulting from aggregating and analysing individuals' publicly surveilled behaviour discloses their psychological propensities and inclinations, then this discloses incredibly intimate details about the individuals that is analogous to their mental health records.

In regard to what is meant by control of information, there can be many cases that fall within a grey area (e.g., control over Internet activity data); but, it is widely acknowledged that intimate information from mental health records can only be released with the consent of the individual or under a court order. Similarly, consent or a court order is required for a mental health professional to produce a psychological profile in the first place. The target of FRS thus loses control over intimate information both when the psychological profile is created and when it is disclosed or sold. Hence, to the degree to which we conceive of privacy as control over intimate information, our initial case seems to coincide with this conception of privacy.

One potential objection is that there is little that is intimate or personal about what one does while in public. Again, it is not the observation of innocuous, individual data points that in themselves violate a person's privacy. It is only when these data points are aggregated and analysed that intimate information about the individual is uncovered. However, the non-anonymous nature of this data makes the control over the intimate information that can be inferred from it vulnerable, and, under this conception, privacy is equated with control over intimate information. In this sense, the protections recommended for preserving anonymity as obscurity in public can readily be interpreted as privacy protections.

Second, if we turn our attention to the potential harms of psychological manipulation and opportunity loss from FRS, obscurity protections against these potential harms overlap with other privacy conceptions. Jeffrey Reiman (1976: 39) conceived of privacy as what protects the integrity of personhood:

> Privacy is an essential part of the complex social practice by means of which the social group recognizes – and communicates to the individual – that his existence is his own. And this is a precondition of personhood. To be a person, an individual must recognize not just his actual capacity to shape his destiny by his choices. He must also recognize that he has an exclusive moral right to shape his destiny.

Reiman claims that, in the absence of privacy, the social group fails to demonstrate respect for the individual's exclusive right to be self-determining regarding both body and thoughts. He suggests that self-ownership is established through the social ritual of communicating respect for privacy. These complex social practices aren't uniform across cultures but, before one can have rights to property or rights over the person, self-ownership of body and thoughts must be socially recognised and communicated. Psychological manipulation enabled by FRS profiling is contrary to respecting the individual's personhood and self-ownership of their own thoughts. For society to communicate to individuals that they have the exclusive right to determine their own destinies, it must establish legal restrictions upon FRS to minimise individuals' vulnerability to psychological manipulation.

One immediate complaint regarding this conception of privacy is that it reduces privacy interests to autonomy or basic liberty interests. This criticism seems to echo Thomson's (1975) claim that privacy lacks independent explanatory power, and privacy claims can be reduced to other more fundamental rights claims. Thomson may be right to the extent that we don't need the right to privacy to explain why people ought to be protected from psychological manipulation. We need only consider the way people's autonomy would be violated by such manipulation to recognise the need for legal protections. Reiman argues in opposition to Thomson that the right to privacy is more fundamental and a precondition for establishing the right to property and rights over the person that Thomson argues all privacy claims can be reduced to:

> The right to privacy is the right to the existence of a social practice which makes it possible for me to think of this existence as *mine*. This means that it is the right to conditions necessary for me to think of myself as the kind of entity for whom it would be meaningful and important to claim personal and property rights [emphasis original]. (Reiman, 1976: 43)

Reiman's counter to Thomson is convincing, *if* we assume Thomson means that privacy can be reduced to an interest in merely not having one's autonomy directly interfered with. (It is not clear to me that this assumption is warranted, as Thomson may be employing a richer notion of autonomy; however, this fine point in the debate is not central to my argument.) As a right to a series of social practices, Reiman's conception of privacy cannot simply be reduced to a protection from direct interference. More central to our concerns, if the aim of privacy rights is only the protection of individual autonomy from direct interference, then this would not protect against the collection of non-anonymous FRS data nor restrict the creation of psychological profiles but only protect against the use of the profiles to directly manipulate individuals. In contrast, Reiman's conception of privacy as a complex social practice whereby recognition of self-ownership and autonomy is communicated to members of the group maps more directly with regulations that protect individuals' obscurity while in public from FRS. Reiman's point is that, without communicating their recognition that individuals have an exclusive right to their own thoughts and to be self-directing, the state fails to respect individuals' right to privacy. By not minimising individuals' vulnerability to psychological manipulation, a state would indeed fail to clearly communicate a recognition of every individual's exclusive right to shape their own destiny.

Opportunity loss maps less directly to any common conception of privacy. The creation of profiles that detail individuals' psychological characteristics and behavioural patterns could be used to screen individuals when they apply for jobs, schools, housing, insurance, or public assistance. One interpretation of the interest under threat is that we seek to protect individuals' reputations such that their opportunities are not unfairly limited. Though the connection between reputation protection and privacy is not well theorised, the disclosure of *some* intimate information can be damaging to one's reputation and can lead to opportunity loss. In the absence of adequate privacy protections in general, people's reputations and opportunities will certainly be vulnerable. Just as we sometimes value privacy as a means to protect individuals' reputations, we can value our obscurity in public for concerns over reputation and opportunity loss. Thus, even if protecting our obscurity in public for the sake of avoiding unjust opportunity loss does not seamlessly coincide with privacy claims, such protections do correspond to conceptions of privacy that are linked to protecting reputation.

Unlike the way FRS can be used to form detailed psychological profiles, cataloguing the participants of public activities does not disclose intimate information about them. Their religious and political affiliations are publicly displayed and can be observed by anyone. Nor does it *directly* make them vulnerable to psychological manipulation or some other way of undermining the individual's ability to shape their own destiny. (Of course, the data from cataloguing people's public participation could be aggregated into a broader profile that could be used to manipulate people's beliefs and actions; however, the cataloguing by itself does not have this potential.) The implicit intimidation produced by such cataloguing of participants does not violate an individual's bodily or mental self-ownership. Cataloguing political and religious participants is not antithetical to the group still communicating the recognition of an exclusive moral right of individuals to the integrity of their personhood. Instead, it fails to communicate to citizens that they are not vulnerable to negative repercussions when they exercise their rights to free speech, assembly, and religious worship. This failure violates the broad interests of liberal democracies, as opposed to the privacy interests of individuals.[5]

In the absence of any clear lines connecting the cataloguing of public participants within political and religious group activities with privacy interests or connecting privacy to the societal values made vulnerable by this surveillance practice, it may be best to view the right to anonymity as obscurity in public as distinct from privacy rights – at least in this context. Given the conceptual disarray privacy suffers from, I do not suggest that the independence of this obscurity interest is definitive. Instead, our interest in preserving anonymity when publicly engaged in protests, political rallies, religious observances, or any socially stigmatised activity can only be tangentially thought of as a privacy concern. The apparent independence of this right to obscurity is not a problem for my argument but indicates that advocacy for policies and laws banning real-time facial recognition to catalogue participants in protests, rallies, religious observances, or socially stigmatised activities ought to be made *without* appealing to privacy, to lessen political resistance to establishing policy and law that will protect societies from the harms imposed by real-time FRS.

Conclusion

When considering non-augmented CCTV, there has been significant resistance in the literature to claims that widespread video surveillance violates people's privacy or that such public surveillance wrongs individuals in some other way. It has been argued (Alfino et al., 2003) that, if those being surveilled via CCTV are unaware of being observed or recorded, then their autonomy is not negatively affected, nor can we claim a right to not be observed while in public (Ryberg, 2007). Nissenbaum's (1998, 2010) work on privacy in public has helped to show that privacy interests are not limited to what happens in the "private realm". While she convincingly argues that individuals can be wronged when the contextual integrity of their data is not preserved – and that this holds for data mined from public or Internet activities as much as from more private settings – this does not capture what is new about FRS.

The integration of facial recognition programs into our already extensive video surveillance infrastructure – as well as it being deployed in police body cameras and drones – promises to eliminate our anonymity as obscurity in public. It is precisely this loss that is novel about this technological development. Some might associate their unease with this development with a violation of privacy, but anonymity and privacy are not the same thing. Anonymity involves dissociating the identity of the person from some information about them. Anonymising data can be a means of preserving privacy interests but, as examples like anonymous peer review show, anonymity can serve other ends besides privacy. In addition, the anonymity of being a mere face in the crowd can be valuable in itself, though this liberating value is not sufficient to ground an unconditional right to obscurity while in public.

I have made the case that we have a right to maintain our anonymity such that our mundane activities, behaviours, and associations are not recorded and linked to our identity by means of FRS. The mere collection of this non-anonymous data makes us vulnerable to significant harms in the forms of psychological manipulation and opportunity loss. In addition, I have argued that this right to obscurity is not outweighed by social interests in preventing crime and violence or locating missing persons. These social interests could be equally served while still preserving individuals' anonymity by dissociating location data from personal identities and by only analysing behavioural patterns from anonymous data – until a court order requires the removal of these anonymity protections. Since the risks of psychological manipulation and opportunity loss could be greatly reduced by maintaining these protections to public anonymity, implementing FRS without protecting people's anonymity as obscurity in public would impose unnecessary – and, thus, unjust – risks of harm.

I have also made the case that we have a right to obscurity in public when we are engaged in political, religious, or socially stigmatised activities. The implicit intimidation generated by the state or its law enforcement agencies cataloguing such participation would have a chilling effect, but it may not qualify as direct interference with people exercising their rights to self-expression, assembly, and worship. Merely observing and cataloguing participants is not the same thing as stopping them from protesting. I have argued that the right to anonymity as obscurity is here grounded in the broader societal interest within liberal democracies that individuals can effectively exercise their civil liberties. The implicit intimidation arising from using FRS to catalogue political and religious participants fails to communicate to individuals that they are not vulnerable to the state's power to impose negative repercussions for their activities and convictions.

Given the power asymmetry between those under surveillance and the institutions carrying out the surveillance, the state has a special obligation to reassure individuals that they will not be subject to negative repercussions when they exercise their rights to free speech, assembly, and worship. Reassurance here can only take the form of banning the use of real-time FRS to catalogue participants in political, religious, or socially stigmatised activities. This second right to obscurity in public is also not overridden by competing social interests. The only justifying purpose for such cataloguing is for the sake of a criminal or legal investigation and, for such instances, real-time FRS is not required. A warrant can be required to apply this technology post factum to the video recordings.

If we recognise these two rights to anonymity as obscurity in public, how radically will this alter how we conceive of privacy? This question proves difficult to answer given the conceptual disarray surrounding privacy. However, I have shown that protection against collecting non-anonymous FRS data that can so easily be aggregated and analysed into detail psychological profiles maps closely to two popular conceptions of privacy: control over intimate information and protection of the integrity of the person. That these obscurity and privacy interests coincide so closely may indicate that anonymity is here a means of protecting privacy – but this is a matter for later investigation. On the other hand, it appears that the societal interest in protecting the anonymity of people publicly engaged in political, religious, or socially stigmatised activities is not readily connected to privacy interests. The apparent independence of this right to obscurity is not a problem for my argument but indicates that advocacy for protections against using real-time FRS to catalogue participants in protests, rallies, religious observances, or socially stigmatised activities ought to be made without appealing to privacy to avoid muddying the waters.

Acknowledgements

I would like to thank the participants of the Association for Political Theory Workshop on Interpreting Technology and the ECPR Panel on Big Data, Mass Surveillance and Social Control for their helpful comments on earlier versions of this chapter.

References

Alfino, M., & Mayes, G. R. (2003). Reconstructing the right to privacy. *Social Theory & Practice*, *29*(1), 1–18. https://www.jstor.org/stable/23559211

Al Shouk, A. (2019, March 18). How Dubai's AI cameras helped arrest 319 suspects last year. *Gulf News*. https://gulfnews.com/uae/how-dubais-ai-cameras-helped-arrest-319-suspects-last-year-1.62750675

Botsman, R. (2017, October 21). Big data meets big brother as China moves to rate its citizens. *Wired*. http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Buolamwin, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification Proceedings of the 1st Conference on Fairness, Accountability. In *Proceedings of Machine Learning Research*, *81*, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Burgess, M. (2018, May 4). Facial recognition tech used by UK police is making a ton of mistakes. *Wired, UK*. https://www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival

Del Greco, K. J. (2017, March 22). *Law enforcement's use of facial recognition* [Statement Before the House Committee on Oversight and Government Reform, Washington, D.C.]. FBI. https://www.fbi.gov/news/testimony/law-enforcements-use-of-facial-recognition-technology

Denyer, S. (2018, January 7). China's watchful eye. The *Washington Post*. https://www.washingtonpost.com/news/world/wp/2018/01/07/feature/in-china-facial-recognition-is-sharp-end-of-a-drive-for-total-surveillance/

European Commission. (2021). *Proposal for laying down harmonised rules for the regulation of Artificial Intelligence* (SEC(2021) 167 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=PI_COM:SEC(2021)167&from=EN

European Parliament. (2016). *General data protection regulation* (Regulation (EU) 2016/679). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Fried, C. (1968). Privacy. *The Yale Law Journal*, *77*(3), 475–493. https://www.jstor.org/stable/794941

Friedersdorf, C. (2013, March 28). The horrifying effects of NYPD ethnic profiling on innocent Muslim Americans. *The Atlantic*. https://www.theatlantic.com/politics/archive/2013/03/the-horrifying-effects-of-nypdethnic-profiling-on-innocent-muslim-americans/274434/

Goodin, R. E. (1985). *Protecting the vulnerable: A reanalysis of our social responsibilities*. University of Chicago Press.

Harmon, A. (2019, July 8). As cameras track Detroit's residents, a debate ensues over racial bias. *The New York Times*. https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html?smid=url-share

Harwell, D. (2018, April 26). Facial recognition may be coming to a body camera near you. *The Washington Post*. https://wapo.st/2vN7CPr?tid=ss_mail&utm_term=.d955165fd135

Henschke, A. (2017). *Ethics in an age of surveillance: Personal information and virtual identities*. Cambridge University Press. https://doi.org/10.1017/9781316417249

Inness, J. C. (2003). *Privacy, intimacy and isolation*. Oxford University Press. https://doi.org/10.1093/0195104609.001.0001

Kaste, M. (2018, May 22). Orlando police testing Amazon's real-time facial recognition. *NPR*. https://www.npr.org/2018/05/22/613115969/orlando-police-testing-amazons-real-time-facial-recognition

Laperruque, J. (2017, October 20). Preserving the right to obscurity in the age of facial recognition. *The Century Foundation*. https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/

Lin, L., & Purnell, N. (2019, December 6). A world with a billion cameras watching you is just around the corner. *The Wall Street Journal*. https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402

Manson, N., & O'Neill, O. (2007). *Rethinking informed consent in bioethics*. Cambridge University Press.

Marmor, A. (2015). What is the right to privacy. *Philosophy & Public Affairs*, *43*(1), 3–26. https://doi.org/10.1111/papa.12040

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*(5/6), 559–596. https://www.jstor.org/stable/3505189

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Overgaard, S. (2019, October 21). *A soccer team in Denmark is using facial recognition to stop unruly fans*. NPR. https://www.npr.org/2019/10/21/770280447/a-soccer-team-in-denmark-is-using-facial-recognition-to-stop-unruly-fans

Ponesse, J. (2014). The ties that blind: Conceptualizing anonymity. *The Journal of Social Philosophy*, *45*(3), 304–322. https://doi.org/10.1111/josp.12066

Posner, R. A. (1981). *The economics of justice*. Harvard University Press.

Rachels, J. (1975). Why privacy is important. *Philosophy & Public Affairs*, *4*(4), 323–333. http://www.jstor.org/stable/2265077

Reiman, J. H. (1976). Privacy, intimacy and personhood. *Philosophy & Public Affairs*, *6*(1), 26–44. http://www.jstor.org/stable/2265060

Roos, F., & Källström, L. (2020, Oct. 26). *Facial recognition technologies from a Swedish data protection perspective*. International Network of Privacy Law Professionals. https://inplp.com/latest-news/article/facial-recognition-technologies-from-a-swedish-data-protection-perspective/

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump consultants exploited the Facebook data of millions. *The New York Times*. https://nyti.ms/2GB9dK4

Ryberg, J. (2007). Privacy rights, crime prevention, CCTV and the life of Mrs. Aremac. *Res Publica*, *13*(2), 127–143. https://doi.org/10.1007/s11158-007-9035-x

Skelton, S. (2021, February 18). *Swedish police fined for unlawful use of facial-recognition app*. Computer Weekly. https://www.computerweekly.com/news/252496545/Swedish-police-fined-for-unlawful-use-of-facial-recognition-app

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Swedish Data Protection Agency. (2019). *Supervision pursuant to the general data protection regulation (EU) 2016/679 – facial recognition used to monitor the attendance of students*. (DI-2019-2221). https://www.imy.se/globalassets/dokument/beslut/facial-recognition-used-to-monitor-the-attendance-of-students.pdf

Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs*, *4*(4), 295–314. http://www.jstor.org/stable/2265075

Van Den Haag, E. (1971). On privacy. In J. R. Pennock, & J. W. Chapman (Eds.), *Privacy & personality* (pp. 149–168). Routledge. https://doi.org/10.4324/9781315127439

Vélez, C. (2021). *Privacy is power: Why and how you should take back control of your data*. Melville House.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

Yle News. (2021, April 23). *Finnish police denied, the admit using controversial facial recognition app*. https://yle.fi/uutiset/osasto/news/finnish_police_denied_then_admitted_using_controversial_facial_recognition_app/11899325

Endnotes

[1] I do not focus on the reasonable concerns over the inaccuracy of current facial recognition technology. In a study by the FBI, their facial recognition system produced false positives 15% of the time and only found an accurate match for the other 85% within the top-50 suggested matches (Del Greco, 2017). A study has also shown that the accuracy of facial recognition varies depending upon ethnicity and gender (Buolamwini et al., 2018). While false positives can easily wrong those targeted by this technology, I am generally concerned with whether people are wronged by the institutional practice of FRS.

[2] As the recent Covid-19 lockdowns illustrate, it is conceivable that people's online activity can far out-measure their public activities. However, under more normal circumstances, this will not be the case, on average.

[3] The chilling effects of surveillance in general on free speech, free assembly, and free religious practice is easily observed. For example, when it became known that the New York City Police Department had video cameras aimed at Mosques after the 9/11 attacks, the number of people attending services, classes, and other events at the Mosques dropped dramatically (Friedersdorf, 2013).

[4] As an anonymous reviewer pointed out, this duty might be cast in terms of the state's obligation to optimally support citizens' individual autonomy by reassuring citizens that there will be no negative repercussions for exercising their autonomy within legal limits. I am not prepared, however, to defend a claim that states have an obligation to optimise individual autonomy, as opposed to states having an obligation to protect citizens' ability to effectively exercise their civil rights.

[5] Carrisa Vélez (2021) has claimed that privacy has a political value – especially in our current data economy – insofar as it can protect against data holders maintaining vast power asymmetries over data subjects. She argues that such power asymmetries are antithetical to well-functioning liberal democracies. However, insofar as she conceives of privacy as intimate information, and the damage to liberal democracies she describes comes from profiling and manipulating individuals, her account does not make a clear connection between privacy and the societal harms that I argue result from cataloguing people in public who are engaged in group activities.

CHAPTER 3

To see and be seen

Gynaeopticism and platform surveillance in influencer marketing

JOHANNA ARNESSON & ERIC CARLSSON
DEPARTMENT OF CULTURE AND MEDIA STUDIES, UMEÅ UNIVERSITY, SWEDEN

ABSTRACT
The focal point of this chapter is surveillance practices in relation to social media influencers and digital marketing. The aim is to examine how the idea of surveillance can be expanded to include both social and technological aspects that work at individual, peer, and top-down levels. Drawing on examples from the Swedish influencer industry, we discuss and problematise how surveillance can be understood in such a context and how different dimensions of surveillance are manifested, exploited, and contested. The chapter concludes that participatory and gendered peer- and self-surveillance are inherent parts of influencer culture, and that the commercial success of influencers depends upon these practices. Similarly, platform surveillance and data mining connected to digital advertising can be understood as part of a contemporary commercialised surveillance culture that is closely related to both digital technology and the political economy of the influencer industry.

KEYWORDS: influencer culture, surveillance, gynaeopticon, platform surveillance, media monitoring

Arnesson, J., & Carlsson, E. (2023). To see and be seen: Gynaeopticism and platform surveillance in influencer marketing. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), Everyday life in the culture of surveillance (pp. 67–88). Nordicom, University of Gothenburg.
https://doi.org/10.48335/9789188855732-3

Introduction

The notion that we live in a surveillance society (Lyon, 2003) – where different techniques of watching, and of gathering, storing, and reassembling information in new forms are ubiquitous and imbedded in people's everyday lives – raises a range of questions and concerns. One of these is what surveillance means: If surveillance is everywhere and everything, how can it be defined and analysed? Surveillance can be seen as a systematic and focused manner of observing (Dubrofsky & Magnet, 2015), where the collection and use of information is coupled with power (Andrejevic, 2015) with the purpose of influencing and managing those whose data has been collected (Lyon, 2003), and specifically focused on behavioural modification (Zuboff, 2015). Based on this definition, we argue, in line with Andrejevic (2019), that the notion can be understood in several ways, blurring the borders between surveillance and different forms of monitoring in a wide range of social, economic, and political settings.

In this chapter, we discuss and problematise different forms of surveillance in relation to a promotional industry that is characteristic of the contemporary moment: influencer marketing and the culture of social media micro-celebrity (Borchers, 2019; Khamis et al., 2017). How can surveillance be understood in such a context, and what types of surveillance are emerging within the influencer industry? How are different dimensions of surveillance manifested, exploited, and contested? The aim is to examine how the idea of surveillance can be expanded to include both social and technological aspects of social media influencers and digital marketing. We specifically focus on gendered forms of self- and peer-surveillance, as well as top-down data mining and platform surveillance in this context. The chapter engages with scholarly debates on contemporary surveillance practices and theories using empirical examples from the Swedish influencer industry – with a special focus on a group of successful female influencers in the lifestyle, beauty, and fashion genre – as well as the media monitoring and digital advertising industry. Most of the material has been collected through "lurking" on influencer platforms (Ferguson, 2017) as part of an ongoing research project focusing on influencer politics in Sweden (see Arnesson, 2022).

Widening the notion of surveillance

Media users today are subjected to various forms of surveillance enabled by the affordances of social media technology. While surveillance in terms of bureaucratic administration, national security, and crime prevention has played a central role in the organisation of modern society since the early 1900s, the last 20 years have seen an increased focus on diverse ways of monitoring and storing information about individuals and their everyday lives. This development has been largely enabled by technological innovations, digital media, and the widespread use of smartphones (Andrejevic, 2015).

A couple of decades ago, the Internet was regarded by many as a sphere where individuals could "see and not be seen"; surveillance, it was believed, would be impossible in a cyberspace populated by bodiless, "unseeable" users (Nakamura, 2015). This rather optimistic view was prevalent during the early 2010s, for example, when social network sites were described as "autonomous spaces" where political activists could form networks of change without fear of surveillance or repercussions (Castells, 2012). As Nakamura (2015: 224) points out, however, the development of social media has led to a situation where, rather than being invisible, media users have become "more visible and trackable than ever". Simultaneously, states that seek to control and discipline citizens are no longer the sole practitioners of surveillance; mediated monitoring is increasingly important for commercial organisations and the digital marketing industry. Social media users are supposed to constantly post images, comment, like, subscribe, follow, and in different ways express themselves in and through digital media – practices that generate large quantities of personal data about their lives, dreams, and needs. This data has, in turn, become a goldmine for a variety of commercial actors.

The meanings of surveillance have also widened to include modes of watching that emerge from the engagement of users. A common trope in surveillance studies has been the panopticon model deriving from the late eighteenth-century philosopher Jeremy Bentham's dream of a self-regulatory prison architecture. In Foucault's (1977) *Discipline and Punish*, the panopticon is described as an ideal system for control and knowledge production in institutions such as prisons, schools, factories, and even cities. The idea was that when bodies were placed within a field of visibility, power and coercion would become more efficient, since (to avoid repression by their inspectors) the surveilled subjects would simultaneously become their own overseers, adapting themselves to the ruling norms.

While this understanding of surveillance – as a form of power system strongly related to the notion of self-discipline, visibility, and fixed places – is still important, other modes of more fluid and social forms of surveillance have since been developed by theorists and surveillance scholars. The feminist researcher Rosalind Gill (2019) highlighted how questions of peer- and self-surveillance are increasingly important in contemporary society, not least in digital media cultures that build on voluntariness and collaboration. These modes of surveillance emerge from the participatory practices of media users and function at a peer-to-peer level, as well as through self-disciplinary practices.

Drawing on the work of Alison Winch (2013, 2015), we consider surveillance to be an important feminist issue, since different modes of watching have always been a way to control and regulate women – for example, through the "male gaze" in film and popular culture (Mulvey, 1989) – and this might create an internalised gaze focused on both oneself and other women. From this perspective, the participatory culture of digital media creates a gynaeopticon – a gendered, neoliberal variation on the panopticon – where "the many women watch the many women" (Winch, 2015: 229). The gynaeopticon builds on a tightly bound community of peer-surveillance, and a range of digital self-surveillance practices such as self-tracking devices, beauty apps, and photo filters (Gill, 2019). In the first part of this chapter, we discuss how these gendered forms of surveillance are inherent to influencer culture, and how they also contribute to post-feminist commercial success.

Influencer marketing also involves more top-down surveillance practices, such as the gathering and storing of user information for commercial purposes, practices made possible through the technological affordances of platform surveillance (Wood & Monahan, 2019). Shoshana Zuboff (2015) describes this newer kind of surveillance as part of an omnipresent surveillance capitalism based on data mining. Digital advertising and influencer marketing are not exceptions: Keeping track of user data and follower engagement is a driving force for both influencers and their collaboration partners.

The centrality of platform surveillance also generates imaginative visions of the future within the industry, where new legislation and technological innovation can lead to both the disruption and evolution of surveillance practices. Sociotechnical imaginaries (Jasanoff, 2015) as a concept focuses on the role of technologies in shaping the social fabric of everyday life. According to Jasanoff (2015: 332), these imaginaries are "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology". In the last part of this chapter, we exemplify and discuss how new technology is envisioned as a set of monitoring tools in the digital marketing industry.

Influencers and influencer marketing

Although the term influencer has become globally ubiquitous during the last decade, there is still a certain vagueness about what it really means. A general definition characterises influencers as individuals who display a narrative of their personal lives on social networking platforms or in personal blogs, and who, in different ways, interact with and capitalise upon the audience they accumulate through these platforms (Abidin, 2015). The genre of lifestyle and fashion influencers upon which we focus here has emerged from digital participatory practices such as blogging, where regular people shared their passion for fashion and built online fame by promoting themselves and collaborating with others (Duffy, 2015). Although ideals such as amateurism, authenticity, and autonomy still underpin many influencers' self-presentations, the phenomenon has undergone rapid professionalisation, and the industry has expanded to include not just micro-celebrities and their commercial partners, but also intermediaries such as agents, editors, and the media-monitoring business (Stoldt et al., 2019).

Interest in influencers has grown substantially over the past decade, in both commercial and academic contexts. Research in strategic communication shows, for example, that influencer marketing has created new ways for companies and brands to reach established or potential audiences (Borchers, 2019; De Veirman et al., 2017; Freberg et al., 2011; Hudders et al., 2021; Ye et al., 2021). Creating a strong relationship with your audience by integrating advertising and personal stories has also been highlighted as an effective way to market both products and people (Lueck, 2015).

> Influencer Marketing is one of the fastest-growing and most successful marketing methods worldwide. By being a global multi-billion-dollar industry, the channel has proven to be a key factor in enabling companies and brands to grow and establish themselves much faster than just a few years ago. The methodology behind influencer marketing is based on our behaviour of preferring recommendations from like-minded people over those we receive through traditional advertising. (Cure Media, 2021: para. 1–2)

The excerpt above, taken from the Swedish influencer marketing agency Cure Media, describes influencer marketing as one of the more lucrative strategies for marketing today. It is a form of advertising aimed at influencing the purchasing behaviour of followers and their desire for various types of products, brands, and lifestyles. This is accomplished through digital advertising on the influencer's social media profiles and platforms, as well as through branded content in the form of "collaborations" between the influencer and their partner brand.

Influencer marketing is also seen as a cost-efficient marketing tool because it is not always perceived as advertising by followers (Ye et al., 2021). The parasocial relationship between influencers and their followers, based on interaction and sharing personal information, facilitates feelings of belonging and social connectedness that are often perceived as a form of friendship (Arnesson, 2022; Breves et al., 2021; Lueck, 2015; Pöyry et al., 2019). To predict and measure behavioural intentions, followers' interactions on social media are mined, monitored, and analysed on a huge scale for commercial purposes. The relationship is therefore not as equal as it might seem: Since the followers are a prerequisite for influencers' commercial success, they constitute the "audience commodity" that influencers sell to advertisers and collaboration partners (Hunter, 2016). This is achieved by means of different monitoring techniques and surveillance practices, which are further discussed later in this chapter.

Gynaeopticism and the girlfriend gaze in influencer culture

Although different forms of surveillance are prevalent today in most people's everyday lives, some of us become objects of monitoring to a greater degree than others, or in specific forms and contexts. In the following sections, we present and discuss some examples of gendered social surveillance in influencer culture and marketing – examples that are made possible through the specific affordances of social media.

The genre of female micro-celebrities upon which we focus here can be understood as digital representatives of "girlfriend media", that is, magazines marketed to women that position themselves as friends to the reader, giving loving advice at the same time as certain ideals (e.g., slenderness) are reinforced and celebrated. In a Swedish context, magazines such as *Frida*, *VeckoRevyn*, *Amelia*, and *Elle* are all representative of the genre, with advice on fashion, appearance, health, beauty, and love being offered to both teenage girls and older women. Such advice is often presented in collaboration with the fashion and beauty industries, which thrive on women's regulatory gaze upon themselves and others. Their ubiquitous tips and guidance about how to discipline and transform the female body are often disguised in girlfriend rhetoric (Winch, 2013).

Like girlfriend media, influencer culture is saturated by both intimacy and scrutiny; the close affective relationship between influencer and followers mimics a form of female friendship in which girls (and women) control and discipline each other based on normative notions of beauty, femininity, and morals. Just as in other popular culture marketed to women, the body of the influencer is positioned as an object of scrutiny and anxiety – an object of both desire and critique. It is also an object of transformation and improvement in different ways. In addition to "ordinary" beauty treatments and makeup practices, non-surgical cosmetic procedures such as Botox injections that smooth out wrinkles, or "fillers" that plump and shape the lips, are becoming increasingly normalised and socially accepted – a development partially enabled by collaborations between clinics and popular influencers.

In a postfeminist culture where women's online self-representation is framed as empowering, giving them agency over their image and identity-making, the body (and representations of bodies) becomes a tool for self-expression and empowerment (Gill, 2019). In contrast to the "traditional" notion of the male gaze in film (Mulvey, 1989), digital visual culture positions women as active subjects and producers of their own "to be looked at-ness", rather than as passive objects of another's gaze (Dubrofsky & Wood, 2015). It also enables gynaeopticism and a "girlfriend gaze" (Winch, 2013) that is not necessarily about being attractive to men, but rather about being attractive to other women who possess the interest and expertise to recognise the time and labour that goes into the maintenance of a normative body, femininity, and sexuality.

While we focus on gendered peer-surveillance in this chapter, it is important to point out that normative understandings of beauty, appearance, and agency in the influencer industry and other girlfriend media are often impacted by intersecting power structures that configure a range of subject positions in different ways. Monitoring and commenting on female bodies might, for example, be both racialised and sexualised (Dubrofsky & Wood, 2015). Recent years have also seen an upsurge in similar advice directed towards men and masculinity, since the industry is starting to tap into this previously unexploited market. There are, however, still very few male equivalents to girls' and women's magazines, and almost no men (either as influencers or followers) in the Swedish fashion, beauty, and lifestyle influencer industry (Price, 2022).

Entrepreneurial femininity and forensic dissection

The recent upsurge in social media influencers, who build their online presence through self-branding and entrepreneurial femininity, is an example of how being looked at can generate both fame and wealth in digital media (e.g., Abidin & Gwynne, 2017; Archer, 2019; Duffy & Hund, 2015; Duffy & Pruchniewska, 2017; Genz, 2015). In the postfeminist gynaeopticon, the female body is an object of labour: an asset and a product that can be managed and developed into a personal brand that becomes "a gateway to freedom and empowerment" within the neoliberal market economy (Winch, 2015: 233). Such labour is, of course, not new to the contemporary moment, nor is it unique to influencers – it has been used by female celebrities for decades (e.g., Madonna in the 1980s) and is crucial for social media celebrities as well as "ordinary women" who invest in their looks as a form of "beauty capital" and a means to accumulate money, power, and status (e.g., Laurén, 2021). In contemporary beauty culture, however, this form of labour is often glossed over as "me-time" or "self-care": self-improving practices that all women – not just celebrities – are presumed to deserve and enjoy, which simultaneously raises the bar for what is an acceptable and expected female appearance.

Similarly, the way in which women are invited to look at themselves and others through a normative, regulatory gaze has been a characteristic of women's magazines for many years (e.g., Winship, 2000). However, new digital tools and social practices have enhanced the ways in which the female body is looked upon and scrutinised in and through mediated images and marketing. The affordances of social media enable what Gill (2019: 155) calls forensic dissection – a form of gendered peer- and self-surveillance "operating at ever finer-grained levels and with a proliferating range of lenses". Women, especially younger generations, are increasingly subjected to social media content that effectively erases all traces of imperfection – for example, less-than-"flawless" skin – but they are also increasingly aware of how such effects are made possible by photo filters and digital editing, as well as the importance of angles and lighting in photography. Digital tools simultaneously inform users of the curated nature of social media representations and create new standards of appearance based on these possibilities. The beauty and makeup industry, for example, mimics the idea of digital editing by promoting products such as No7 "Airbrush Away Pore Minimising Primer" or the "Photo Finish Pore Minimizing Primer" from Smashbox.

Self- and peer-surveillance in influencer marketing

The girlfriend gaze, and forensic forms of looking at oneself and others, is woven into the fabric of influencer culture and marketing in several ways, exemplified here by the self and peer surveillance practices that contribute to gynaeopticism, generating both conflict and commercial success. As discussed earlier, traditional girlfriend media often position themselves as the ones looking at other women or encourage readers to look at themselves. Influencers, however, also invite others to look at *them*: Being noticeable through their own self-presentation is part of the labour of visibility that aspiring influencers perform to gain and maintain attention and followers (Abidin, 2016).

Being looked at – and looking at oneself – is also an important aspect of commercial collaborations between influencers and beauty brands, since, to a large extent, these build on the influencer's own use of and judgement about certain products. Forensic dissection of one's own appearance – specifically commenting on perceived flaws and problem areas – thus becomes part of the authenticity work that influencers perform to present themselves as relatable to their followers. When the cookbook author and lifestyle influencer Sofia Wood collaborates with the skincare brand Mantle, for example, her posts are frequently illustrated by close-up photos of her face and include detailed accounts of problematic aspects of her skin – dryness, redness, flaking, and so on (e.g., Wood, 2021). By inviting this close inspection of herself, she becomes relatable to her followers, constructing an "aspirational extra/ordinariness" (McRae, 2017) that reinforces both the notion that women need to scrutinise their appearance for flaws and the belief that such flaws can be corrected by following the influencer's example in terms of beauty routines and products.

Forensic looking is also characteristic of the discussions in the comments sections of influencers' own blogs and Instagram profiles. The affordances of such platforms encourage engagement, interaction, and ongoing scrutiny of – and debate about – the influencer's lifestyle, consumption, and appearance. It is not uncommon for influencers to be asked questions about certain details in a photo, for example, an item in the background, the brand of a lipstick, or the exact colour of a wall paint. The girlfriend gaze of followers is fixed on the influencer's representations of herself and her life in both image and text, often coupled with an extensive knowledge of her habits, preferences, values, and aesthetics.

Being looked at by a wide range of actors – followers, haters, other influencers, the media, and so on – is, from this point of view, a prerequisite for the kind of micro-celebrity upon which influencer marketing builds. As Lyon (2003: 164) warns, however, "surveillance is always Janus faced": It is the close monitoring of an influencer's life and relationships (presented as "engagement") that makes them relevant to advertisers, collaboration partners, and followers – at the same time as this constant scrutiny can be difficult to manage, especially when increasingly blurred borders between privacy and publicity are so inherent to the influencer profession.

An example of such tensions and blurred borders can be found in the case of Sandra Beijer, a "first-generation" Swedish influencer who started her social media career over a decade ago. In addition to a career in advertising and as a writer, she has predominantly built her self-brand around partying, travelling, romantic relationships, and not conforming to social norms about appropriate life priorities or fashion styles for women, specifically as she passed the age of thirty. Thus, comments urging her to "grow up" and "act her age" have been a recurring feature on her blog and social media profiles, and the issue of motherhood has also been discussed in relation to her non–family-oriented lifestyle. While Beijer never explicitly said that she did not want to have children, many of her long-term followers have certainly had that perception of her. It was, therefore, somewhat surprising to many when rumours that she was pregnant started to float around the Internet in early 2021. On 23 May, she finally revealed that these rumours were true by posting a series of photos on her blog that clearly show her pregnancy, accompanied by the short remark "yes, it's a baby" (Beijer, 2021).

Many speculations about Beijer's presumed pregnancy were based on detailed scrutiny of the content that she produced during this time, especially photos. Followers pointed out "proof", such as the lack of alcoholic beverages in images from nights out, that Beijer's clothing style and appearance had changed ("I can see it in your face"), and that she only posted pictures of herself from certain angles or that were cropped in certain ways. It is clear that this scrutiny was stressful for her at a personal level: It is a topic in several blogposts where Beijer calls out followers for posting unwanted comments about her body, clothes, and habits during her early pregnancy – comments that she had to delete to retain some degree of privacy. At the same time, it is this kind of follower attention to detail and assemblages of information that makes Beijer so successful, since the engagement of followers also signifies their perceived interconnectedness and her influence upon them.

Gossip and meta-blogging as peer-surveillance

The discussion about Beijer's pregnancy was also prominent on *Bloggbevakning*; a Swedish website whose name literally means "blog monitoring" in English. This name might sound a bit archaic but should be perceived as a testament to the site's long lifespan rather than its actual focus. Most of the content and discussions today centre upon influencers' posts and interactions on platforms such as Instagram and TikTok, in addition to "the blogosphere". The caption on the blog states that it is "a blog about bloggers and social media" and, according to its own Instagram account, it has two million visitors per month (Bloggbevakning, 2021a).

The editor Camilla Gervide launched *Bloggbevakning* as her own private blog, although today it is hosted by *Nyheter24*, an online news site primarily targeting women aged 25–44 and which is part of the Swedish media house Life of Svea (Life of Svea, 2021). Gervide claims that she started the blog "just for fun" but soon came to believe that "something was crooked in the business", and therefore, the focus shifted to critically examining influencers and their impact on their audiences (Cision, 2021). Today, however, *Bloggbevakning* has converged with the world it set out to scrutinise; for example, it is listed on Ocast, a platform for buying and selling ad space and marketing campaigns on digital media, as a seller of "influencer marketing" for products such as ambassadorship, events, influencer collaborations, and micro-influencer campaigns (Ocast, 2021).

The gathering and storage of information is a prerequisite for the site's popularity: Without its ongoing monitoring of what is happening on the Swedish "influencer scene", it would not be relevant to its readers, whether they are occasional visitors or part of the community that has formed in its comment sections. The information is selected and presented to the audience in a flow of updates, although posts are also stored in the blog's archive, which extends back to its beginnings in 2016. In addition, posts are labelled according to which influencer forms its focus and are compiled under the subheading "Categories" on the site. It is therefore possible to follow a specific influencer for a long period of time and to assemble a large amount of information about their life, appearance, and career.

Monitoring influencers in this way also serves to change behaviour, specifically behaviour that is deemed "unethical" or deceptive by the site's editor. Among these are, for example, vacation trips to exotic places, the marketing of cosmetic surgery, or lack of disclosure when it comes to sponsored content in general. While this scrutiny might have initially had a journalistic ambition – being an outsider looking in – the integration of the site into the Swedish influencer industry, and the development of its editor as an influencer herself, makes it possible to understand such practices as a form of peer-surveillance. Naming and shaming behaviour that is labelled "problematic" is also characteristic of the comment sections, where readers (predominantly women) engage in debate and discussions about the featured influencers, as well as about the blog itself (and the person behind it).

Like other, better-known “hateblogs”, such as *Get off My Internets* – described as “the first blogger/influencer focused gossip website” (GOMIBLOG, 2021) – *Bloggbevakning* has developed its own community, which adheres to specific social norms and ideals. Research suggests that these forums are often characterised by an ongoing deconstruction of influencers’ femininity and authenticity, as well as aggressive or satirical statements on influencers’ appearance, habits, and social media content (Duffy et al., 2022; McRae, 2017). It is clear that influencers know that they are being watched from the way in which they occasionally refer to the blog on their own platforms, or tell readers who post critical comments that, if they feel a need to criticise, they can do so on *Bloggbevakning*. At the same time, attracting attention and being the centre of public discussion is an important factor in the affective economy that underpins influencer marketing, where visibility and fame are the keys to commercial success. The emotional engagement generated by the social surveillance on sites such as *Bloggbevakning* may result in even more attention and new commercial opportunities.

The comments section of *Bloggbevakning* is infamous for its crude tone and “gossipy” culture and, until May 2021, it was almost completely unmoderated. It is a digital sphere where gynaeopticism and the girlfriend gaze can be observed in discussions concerning influencers’ appearance and behaviour, specifically in relation to cosmetic surgery and different beauty treatments. A recurring object of such discussions is Paulina Danielsson, better known under her nickname Paow, who has made a name for herself during the last decade as an influencer and reality-TV star. Her social media content is frequently featured on the blog, especially her collaborations with cosmetic surgery clinics in Turkey, where she has undergone several procedures to enhance or change certain features (e.g., Bloggbevakning, 2021b). Posts might be followed by hundreds of comments in which the girlfriend gaze is focused on her appearance before and after surgery. What makes these discussions interesting is the way in which they articulate the community’s ambivalent attitudes towards scrutinising and criticising other women. Some commenters remark on Paow’s “unnatural” appearance, or that she looks “sad” and “tragic” after the procedures. These negative statements are often related to forensic looking and extensive scrutiny of “before and after” pictures of the results, down to very small details in photos. Others question these judgements and instead criticise *Bloggbevakning* for framing the posts in such a way that the discussion becomes a mockery of an individual person, rather than a critique of the cosmetic surgery industry and the beauty ideals that women are invited to internalise.

Platform surveillance in the digital marketing industry

So far, we have discussed how a range of self- and peer-surveillance practices are inherent to influencer culture, and how these also contribute to the commercial success of influencers in the beauty and lifestyle genre. We now continue the chapter by discussing how advanced data monitoring is another necessary condition for the influencer marketing industry. This describes how industry intermediaries collect, analyse, and package the engagement of customers, fans, and followers into a product that can be sold to other commercial actors seeking advertising space for products, brands, and services. When discussing surveillance as data monitoring, it is fruitful to consider how digital environments, rather than social codes, affect the subjectivities of users (and other stakeholders). Such a perspective shifts the focus from Foucault's formulation of visibility as a vehicle for self-discipline and the peer-surveillance of Gill's notion of the gynaeopticon, to prediction of behaviours against the background of the platforms' design, structure, and ability to mine data.

In the monitoring industry, digital environments are designed, one might say, to function as sensors that categorise, collect, and predict user behaviour. An overall way to describe such monitoring is the term platform surveillance (Wood & Monahan, 2019). The platform, seen as a metaphor – a framework connected to other media technologies (interfaces, servers, devices, code, cables, etc.) – can be used, according to Wood and Monahan, to better grasp the infrastructural logic of modern digital media ecosystems and their affordances. As Wood and Monahan (2019: 3) put it:

> The platform has returned to its earliest sense of a framework or, one could also say, an infrastructure. [...] Infrastructures establish contexts for practice. They enable, support, and afford certain practices while necessarily disabling, eroding, and resisting others.

Platform surveillance, they suggest, can be recognised as a kind of "governmentality" (Foucault, 2008). That is, not only networked technological infrastructures and technical information systems whose main function is to collect and analyse user data, but also a radically new form of techno-political economy through which subjects are governed. Apart from data collection, an important purpose of these infrastructures is to push and modify media users' behaviour in one way or another. Many platforms are designed to make their users stay and come back; click, like, and post content; or buy (advertised) products.

Platform surveillance bears some resemblance to Shoshana Zuboff's (2015) broader term, surveillance capitalism, which designates the logic of accumulation invented and embraced by the tech industry. Her argument is that big tech companies (and smaller ones) make profit by turning user engagement into assets, and by doing so, they provide the main source of economic revenue in various markets. Measurement of the performance of online users has been described as the "asset of the 21st century" (Birch et al., 2021: 1). According to these authors, it is the monitoring and measurement of users' behaviour that is made valuable and sold on a market (e.g., how much time they spend, how they click, their repetitive patterns of behaviour, engagement, etc.). The user per se is not what is up for sale, but personal data harvested from users is converted into economic objects that are being tracked and recorded for future monetisation.

Data monitoring, prediction, and sociotechnical imaginaries

Platform surveillance was spearheaded by companies such as Facebook and Google, but the technique is also used by numerous smaller businesses, whose entire economic model is based on tracking, storing, and selling the data that people generate when using media ecosystems such as social networking sites, search engines, web shops, apps, online magazines, and the like. In this section, we present and discuss examples of how media companies in Sweden talk about collected user data and how they value such data as assets. In the example below, taken from the podcast *Nordic Ad Tech Review*, the head of data analytics at Aller Media, a market-leading Swedish publicist in popular media with millions of readers every month, discusses the logic and importance of collecting so-called first-party data from users:

> We'll show relevant ads to our users. It benefits the users; it benefits the advertisers and in the long run it is good for us. To do this, we have two main tracks: the first is to obtain first-party data, which is obtained with consent that is clear to the user. Here is Aller Media, I as a user want to log in here and then enable Aller Media to collect certain types of data from me that will be used for things, for these purposes. It is important to have great transparency with the users. What data do we collect, what do we do with it? What do you do if you no longer want to share data? […] We need to enable and accelerate login for our users. […] We need a first-party data business for our IO business and for our deals [translated]. (Netric Sales, 2021–2022)

Aller Media hosts several of the influencers that we have already discussed above, and the monitoring of readers and followers is explained and justified by the belief that it is good for both the users and the industry – that it benefits everyone involved. This form of "soft surveillance" also takes place when individuals provide various forms of data to commercial companies through smartphone apps, social media platforms, or other everyday digital platforms and gadgets.

The example above illustrates companies' desire to bind their customers with a login to gain access to first-party data to collect for future use, since third-party data is about to be regulated. Third-party data does not result from a relationship of consent between a company and its customers but consists of the exploitation of massive amounts of user data collected from Internet and smartphone users, often but not exclusively with the purpose of personalised, targeted advertising. As a result of public demands to protect the privacy of users, and recent scandals of intrusion into the privacy of millions of Internet users (Cambridge Analytica), the death of third-party data (cookies, location, and demographic data, etc.) has been announced. The tech giant Google has declared plans to phase out the use of third-party data by 2023, and new legislation such as the General Data Protection Regulation in the European Union has addressed the issue (Perrone, 2020). However, according to an interview with *Bonnier News*, the decline of third-party data is not seen as a major problem for the digital marketing industry, because companies will adjust to work more with predictions of future user behaviour:

> "Digital advertising won't die, it just won't be as accurate. At the beginning, the user may see fewer personal ads, but this will be temporary. We'll work more with predictions, instead of knowing as before exactly what the user is interested in based on previous surfing behaviour," says Dilem Güler, business development manager at Bonnier News [translated]. (Ottosson, 2021: para. 11)

While the industry might miss out on some of the economic opportunities of collecting user data due to these new regulations, there are numerous other ways to monitor user behaviour that the industry can utilise, such as device fingerprinting, eye-tracking, and machine learning. The head of programmatics and display at Aller Media explains some of these possibilities they see in the future:

> We have built up a very strong contextual business where we use machine learning and natural language processing and divide our entire inventory into lots of contextual verticals that we can control [translated]. (Netric Sales, 2021)

In another example taken from the web-based industry magazine *AiThority*, the benefits of topic extraction and natural language processing are described. Natural language processing is a form of monitoring technique that is believed to produce more precise knowledge about potential customers' thoughts, how they might behave, and what they are talking about in digital environments:

> Topic extraction is the act of obtaining common themes or topics from a set of data. This can be extremely useful in order to obtain an idea of what your audience is thinking about and is a large part of what NLP [natural language processing] works off of. Within marketing analytics, topic extraction can help you understand what your audience's inten-

> tions or questions are, which, in turn, allows you to better serve their needs. For example, you can leverage NLP to gain an understanding of what customers are discussing on company forums in order to identify common interests and create targeted content for your audience. (Eng, 2020: para. 2)

The examples discussed above reflect some of the sociotechnical imaginaries (Jasanoff, 2015) about the future of Big Data mining that are prevalent in the industry today; they can be seen as glimpses into the dreams and fantasies of commercial agencies that seek to teach computers to interpret human communication and actions online for the sole purpose of predicting consumers' behaviour and preferences. Issues that corporations previously had to ask people about in consumer surveys they now want to harvest automatically in assemblages of information that might create a never-before-seen insight into consumer tastes, behaviours, and desires.

Biosurveillance as part of the affective economy

Even more speculative is the notion of biosurveillance, which has its origins in the field of medicine and the security industry (Nemorin, 2018). Biosurveillance involves the monitoring of various types of biological and physiological data, such as the spread of diseases (e.g., Covid-19) and data related to the environmental crisis or climate change. Nemorin (2018) discusses how hopes and dreams of such surveillance have spilled over into the commercial sector as well. The argument is that the commercial sector aspires to collect biodata from human bodies (behaviours, emotions, activities, movements in time, space, and place, etc.). A concrete, yet imaginative, form of biosurveillance is so-called neuromarketing:

> In simple terms, neuromarketing is the study of how the brain works when a person has to make a purchasing decision. Whether we're talking about emotional or rational decisions, understanding neuromarketing can be of great help for numerous reasons:
>
> - If you know how to reach the customer's subconscious mind, you can communicate at an indirect or more subtle level.
> - Neuromarketing helps you develop a quick rapport with your prospects.
> - You can significantly boost your conversion rates by making your prospective clients feel certain feelings such as curiosity, scarcity, pleasure, or pain.
>
> (Foster, 2020: para. 1–2)

In this example, monitoring is presented in rather imaginative terms insofar as companies seek to enter potential customers' brains at a subconscious level and thus guide them into desirable buying behaviours. Neuromarketing seeks to capture neurophysiological and biometric data, such as eye movements or facial expressions, to steer potential consumers in certain directions. One example is eye tracking as a marketing tool:

> Screen-based eye tracking allows for the recording and analysis of responses to multimedia stimuli. Perform screen-based eye tracking on images, videos, websites, games, software interfaces, 3D environments, mobile phones to provide deeper insights into visual attention. Eye tracking allows you to see things from the perspective of consumers. Whether you're examining product placement, packaging design, advertising, or user experience, eye tracking accurately reveals what grabs attention, what influences purchase behavior, and how consumers engage with your product. This information helps your business become truly customer-centric. (Tobii Pro, 2022: n.p.)

Eye tracking and neuromarketing techniques can be seen as an indication that platform surveillance is not only about collecting digital traces from media users, but they might also serve as an example of the industry's dream of extending the commodification of biological data from users, such as monitoring blood flows in the brain, facial expressions, heart rate, and respiration. In an article in the Harvard Business Review, it is claimed that "the field of neuromarketing, sometimes known as consumer neuroscience, studies the brain to predict and potentially even manipulate consumer behavior and decision making" (Harrell, 2019: Summary, para. 1). Even though such surveillance techniques are not currently widespread, they are predicted to become cheaper and more common. While neuromarketing might arouse the hopes of a more direct route into the minds of consumers, it would probably be imagined as a nightmare by customers who are being exposed to neuromarketing.

Moreover, neuromarketing is a significant part of what Nemorin (2018) calls the "affective economy", that is, a form of commercialism that strives to influence people's consumer behaviour through the notion of emotional appeal, as in the examples above. Even though emotional appeal has been an important ingredient in various forms of advertising media during the last century (ads in the press, telephone, radio, television, etc.), the new possibilities presented by algorithmic and personalised marketing have emerged in digital media environments such as influencer marketing, which, to a large extent, builds upon fantasies of authenticity, relatability, and different forms of intimacy.

Within this affective economy, it is not only media users who are monitored in the industry's visions of the future, but also the influencers themselves. Bishop (2021) writes about what she calls influencer marketing tools, which are a form of automated tool for monitoring the impact of content generated by different influencers from the perspective of the brand stakeholders. Influencer marketing tools provide analyses of public data from social media and algorithmic calculations of specific influencers' impact on a certain brand. Bishop (2021) argues that brand safety is of central concern, and this is also the rationale behind the surveillance that is carried out by marketing stakeholders using influencer marketing tools to identify bad behaviour and fraud by hired influencers. In a Swedish context, there have been some reports of high numbers of "fake followers" recorded for influencers by the influencer marketing tool *follower check* (Nilsson, 2017). The previously successful Swedish influencer Isabella Löwengrip, for example, has seen most of her brand and commercial success crumble during the last few years based on reports of fake followers and less-than-transparent "engagement" accounts (Lundin & Winberg, 2020). While peer-surveillance by followers and other influencers is an inherent part of the affective economy, as discussed earlier in this chapter, surveillance practices that serve to monitor and regulate influencers seem to be increasingly important in the relationship between influencers and their commercial partners as well.

Conclusions

Surveillance can be understood in many ways in contemporary society, where different modes of watching and seeing, and of gathering and storing information about individuals' everyday lives, arguably serve specific purposes for a range of actors. In this chapter, we have examined what could be called the "sociotechnical imaginaries" of surveillance and how the notion of surveillance can be expanded to include both the social and technological aspects of social media influencers and digital marketing. As we have tried to show in this chapter, imaginaries of technology are rendered in optimistic ways from the perspective of the influencer industry (including digital marketing). However, there are also more pessimistic or critical accounts of imaginaries of the normative relationship between technology and surveillance, as well as the role of technology and "girlfriend media" in shaping gender identities and power relations. We have specifically discussed gendered forms of self- and peer-surveillance, as well as top-down data mining and platform surveillance in this context.

A common characteristic of both gynaeopticism and the surveillance of user data gathered by platforms is that it depends, to a certain extent, on the participation of social media (prod)users, who, through the affordances of digital media, engage in practices that make new forms of surveillance possible. These social and technological surveillance practices are also a prerequisite for success in the industry, for both individual influencers and digital advertising companies. Influencer marketing has grown to be a cultural and economic phenomenon during the last decade, specifically within the beauty and lifestyle industry that particularly targets women. This makes the emerging surveillance cultures of influencer marketing an interesting case from both feminist and political-economy perspectives on the character and impact of online surveillance.

Our examples, taken from the Swedish influencer industry, show that gendered social surveillance is an inherent part of influencer culture, and something that both causes conflict and underpins commercial success. Influencer marketing is situated within a context where the promotional interests of the fashion and beauty industry are coupled with postfeminist notions of emancipation and empowerment through entrepreneurial femininity and self-expression: an ideological construct that both encourages and challenges the "girlfriend gaze" that women are socialised into adopting when looking at themselves and others. Regulatory discourses on femininity and the body, as well as the forensic dissection of visual influencer content, are integral parts of the industry and the social practices that generate online fame. At the same time, the participatory culture of comments sections and meta-discourses around popular influencers show that gynaeopticism can be both reinforced and contested on these platforms.

The imaginaries relating to monitoring thoughts, social relationships, behaviours, conversations, and actions in digital environments – and perhaps, above all, relating to obtaining knowledge and predictions about future relationships and actions – seem to be another important aspect of platform surveillance in this context. The industry promises that – out of the collection and monitoring of data from digital platforms and bodies – there will arise more mapping, refined predictions, and greater influence over individual consumers' behaviour. There seems to be a notion that information gathering is never quite sufficient. More and more comprehensive data monitoring is presented as the key to success. While panoptical surveillance rests on self-discipline and coercion through the gaze of the inspector, this newer kind of "automated surveillance" can be described as an "always-on ubiquitous monitoring, and the implicit understanding that there is always the need for more" (Andrejevic, 2019: 10). Predictions, responses from users, emotional outcomes of content, and biometrics collected from human bodies are therefore lauded as both the driving forces for the ongoing monitoring practices and their legitimation.

Finally, there seems to be another common characteristic that binds together the social and technical aspects of surveillance in the influencer industry: the body, specifically visions of monitoring, using, and shaping the physical appearances and functions of both influencers and their followers. These invasive and corporeal discourses are found in both the gendered social surveillance of gynaeopticism and the utopian (or dystopian) visions of the future within the digital marketing industry – a characteristic that highlights the need for critical research in this area.

Acknowledgements

The research is supported by Vetenskapsrådet [The Swedish Research Council] [2018-01339].

References

Abidin, C. (2015). Communicative intimacies: Influencers and perceived interconnectedness. *Ada: A Journal of Gender, New Media, & Technology* (8). http://dx.doi.org/10.7264/N3MW2FFG

Abidin, C. (2016). Visibility labour: Engaging with influencers' fashion brands and #OOTD advertorial campaigns on Instagram. *Media International Australia*, *161*(1), 86–100. https://doi.org/10.1177/1329878X16665177

Abidin, C., & Gwynne, J. (2017). Entrepreneurial selves, feminine corporeality and lifestyle blogging in Singapore. *Asian Journal of Social Science*, *45*(4-5), 385–408. https://doi.org/10.1163/15685314-04504002

Andrejevic, M. (2015). Foreword. In R. E. Dubrofsky, & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. ix–xviii). Duke University Press.

Andrejevic, M. (2019). Automating surveillance. *Surveillance & Society*, *17*(1/2), 7–13. https://doi.org/10.24908/ss.v17i1/2.12930

Archer, C. (2019). Social media influencers, post-feminism and neoliberalism: How mum bloggers' "playbour" is reshaping public relations. *Public Relations Inquiry*, *8*(2), 149–166. https://doi.org/10.1177/2046147X19846530

Arnesson, J. (2022, February 3). "Endorsing a dictatorship and getting paid for it": Discursive struggles over intimacy and authenticity in the politicisation of influencer collaborations. *New Media & Society*. https://doi.org/10.1177/14614448211064302

Beijer, S. (2021, May 23). Så [So]. *Sandra Beijer*. https://sandrabeijer.elle.se/graviditeten/sa-2/

Birch, K., Cochrane, D., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, *8*(1). https://doi.org/10.1177/20539517211017308

Bishop, S. (2021). Influencer management tools: Algorithmic cultures, brand safety, and bias. *Social Media + Society*, *7*(1). https://doi.org/10.1177/20563051211003066

Bloggbevakning. (2021a). *bloggbevakning* [*blog monitoring*]. Retrieved December 12, 2021, from https://www.instagram.com/bloggbevakning/

Bloggbevakning. (2021b). *Kategori: Paow* [*Category: Paow*]. Retrieved January 30, 2022, from https://nyheter24.se/bloggbevakning/category/paow/

Borchers, N. S. (2019, August 8). Editorial: Social media influencers in strategic communication. *International Journal of Strategic Communication*, *13*(4), 255–260. https://doi.org/10.1080/1553118X.2019.1634075

Breves, P., Amrehn, J., Heidenreich, A., Liebers, N., & Schramm, H. (2021). Blind trust? The importance and interplay of parasocial relationships and advertising disclosures in explaining influencers' persuasive effects on their followers. *International Journal of Advertising*, *40*(7), 1209–1229. https://doi.org/10.1080/02650487.2021.1881237

Castells, M. (2012). Networks of outrage and hope: Social movements in the internet age. Polity.

Cision. (2021). *Bloggbevakning.se – bloggen som granskar influencers* [*Bloggbevakning.se – the blog that scrutinises influencers*]. Retrieved December 20, 2021, from https://www.cision.se/artiklar-och-tips/podcasts/bloggbevakning-se-bloggen-som-granskar-influencers/

Cure Media. (2021). *What is influencer marketing?* https://www.curemedia.com/what-is-influencer-marketing/

De Veirman, M., Cauberghe, V., & Hudders, L. (2017). Marketing through Instagram influencers: The impact of number of followers and product divergence on brand attitude. *International Journal of Advertising*, *36*(5), 798–828. https://doi.org/10.1080/02650487.2017.1348035

Dubrofsky, R. E., & Magnet, S. A. (2015). Feminist surveillance studies: Critical interventions. In R. E. Dubrofsky, & S. A. Magnet (Eds.), *Feminist surveillance studies*. Duke University Press

Dubrofsky, R. E., & Wood, M. M. (2015). Gender, race, and authenticity: Celebrity women tweeting for the gaze. In R. E. Dubrofsky, & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 93–106). Duke University Press.

Duffy, B. E. (2015). Amateur, autonomous, and collaborative: Myths of aspiring female cultural producers in Web 2.0. *Critical Studies in Media Communication*, *32*(1), 48–64. https://doi.org/10.1080/15295036.2014.997832

Duffy, B. E., & Hund, E. (2015). "Having it all" on social media: Entrepreneurial femininity and self-branding among fashion cloggers. *Social Media and Society*, *1*(2). https://doi.org/10.1177/2056305115604337

Duffy, B. E., Miltner, K. M., & Wahlstedt, A. (2022). Policing "fake" femininity: Authenticity, accountability, and influencer antifandom. *New Media & Society*, *24*(7), 1657–1676. https://doi.org/10.1177/14614448221099234

Duffy, B. E., & Pruchniewska, U. (2017). Gender and self-enterprise in the social media age: A digital double bind. *Information, Communication & Society*, *20*(6), 843–859. https://doi.org/10.1080/1369118X.2017.1291703

Eng, C. (2020). *Five use cases for natural language processing (NLP) techniques in marketing analytics*. Aithority - AI Technology Insights. https://aithority.com/natural-language/five-use-cases-for-natural-language-processing-nlp-techniques-in-marketing-analytics/

Ferguson, R.-H. (2017). Offline "stranger" and online lurker: Methods for an ethnography of illicit transactions on the darknet. *Qualitative Research*, *17*(6), 683–698. https://doi.org/10.1177/1468794117718894

Foster, T. (2020, January 16). Mind-blowing neuromarketing tricks for your Instagram content. https://www.nichemarket.co.za/blog/industry-experts/neuromarketing-tips-instagram

Foucault, M. (1977). Discipline and punish: The birth of the prison. Penguin.

Foucault, M. (2008). The birth of biopolitics: Lectures at the Collège de France, 1978–1979. Palgrave Macmillan.

Freberg, K., Graham, K., McGaughey, K., & Freberg, L. A. (2011). Who are the social media influencers? A study of public perceptions of personality. *Public Relations Review*, *37*(1), 90–92. https://doi.org/10.1016/j.pubrev.2010.11.001

Genz, S. (2015). My job is me: Postfeminist celebrity culture and the gendering of authenticity. *Feminist Media Studies*, *15*(4), 545–561. https://doi.org/10.1080/14680777.2014.952758

Gill, R. (2019). Surveillance is a feminist issue. In T. Oren, & A. Press (Eds.), *The Routledge handbook of contemporary feminism* (pp. 148–161). Routledge. https://doi.org/10.4324/9781315728346

GOMIBLOG. (2021). *About GOMIBLOG*. Retrieved December 20, 2021, from https://gomiblog.com/about-gomiblog/

Harrell, E (2019, January 23). *Neuromarketing: What you need to know*. Harvard Business Review. https://hbr.org/2019/01/neuromarketing-what-you-need-to-know

Hudders, L., De Jans, S., & De Veirman, M. (2021). The commercialization of social media stars: A literature review and conceptual framework on the strategic use of social media influencers. *International Journal of Advertising*, *40*(3), 327–375. https://doi.org/10.1080/02650487.2020.1836925

Hunter, A. (2016, September 1). Monetizing the mommy: Mommy blogs and the audience commodity. *Information, Communication & Society*, *19*(9), 1306–1320. https://doi.org/10.1080/1369118X.2016.1187642

Jasanoff, S. (2015). Imagined and invented worlds. In S. Jasanoff, & S. Kim (Eds), *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. University of Chicago Press.

Khamis, S., Ang, L., & Welling, R. (2017). Self-branding, "micro-celebrity" and the rise of social media influencers. *Celebrity Studies*, *8*(2), 191–208. https://doi.org/10.1080/19392397.2016.1218292

Laurén, A.-L. (2021). ”Jag är född vacker – och jag har alltid använt mig av det” [“I was born beautiful: And I have always made use of it”]. *Dagens Nyheter*. https://www.dn.se/varlden/jag-ar-fodd-vacker-och-jag-har-alltid-anvant-mig-av-det/

Life of Svea. (2021). *Varumärken* [*Brands*]. Retrieved December 20, 2021, from https://lifeofsvea.se/#varumarken

Lueck, J. A. (2015). Friend-zone with benefits: The parasocial advertising of Kim Kardashian. *Journal of Marketing Communications*, *21*(2), 91–109. https://doi.org/10.1080/13527266.2012.726235

Lundin, J., & Winberg, Y. (2020). Badfluence? Makt, miljoner & halvsanningar i sociala medier [Badfluence? Power, millions & half-truths in social media]. Atlas.

Lyon, D. (2003). Surveillance technology and surveillance society. In T. J. Misa, P. Brey, & A. Feenberg (Eds.), *Modernity and technology* (pp. 161–184). MIT Press.

McRae, S. (2017). “Get off my internets”: How anti-fans deconstruct lifestyle bloggers’ authenticity work. *Persona Studies*, *3*(1), 13. https://doi.org/10.21153/ps2017vol3no1art640

Mulvey, L. (1989). Visual pleasure and narrative cinema. In L. Mulvey, *Visual and other pleasures* (pp. 14–26). Palgrave Macmillan. https://doi.org/10.1007/978-1-349-19798-9

Nakamura, L. (2015). Afterword: Blaming, shaming, and the feminization of social media. In R. E. Dubrofsky, & S. A. Magnet (Eds.), *Feminist surveillance studies* (pp. 221–228). Duke University Press.

Nemorin, S. (2018). Biosurveillance in new media marketing: World, discourse, representation. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-96217-7

Netric Sales (Creator). (2021–2022). *#2 Aller Media Sweden take on data analysis and prebid testing and optimization* [Audio podcast]. Nordic Ad Tech Review. https://poddtoppen.se/podcast/1573436427/nordic-ad-tech-review/2-aller-media-sweden-take-on-data-analysis-and-prebid-testing-and-optimization

Nilsson, T. (2017). Hälften av influencerns följare är fejkade [Half of the influencer’s followers are fake]. *Resumé*. https://www.resume.se/kommunikation/media/halften-av-influencerns-foljare-ar-fejkade/

Ocast. (2021). *Influencer marketing _ Bloggbevakning*. https://ocast.com/se/bloggbevakning/

Ottosson, M. (2021, July 7). *Tredjepartscookies – vad är det och hur påverkar det dig*? [*Third-party cookies: What are they and how do they affect you?*]. Internetstiftelsen. https://internetstiftelsen.se/nyheter/tredjepartscookies-vad-ar-det-och-hur-paverkar-det-dig/

Perrone, M. (2020). The end of third-party data – Finally. *Forbes Magazine*. https://www.forbes.com/sites/theyec/2020/10/01/the-end-of-third-party-data---finally/?sh=52ce06103f05

Price, A. (2022). Brist på manliga influencers – detta innebär det för marknadsföringen [Lack of male influencers: This is what it means for marketing]. *Resumé*. https://www.resume.se/marknadsforing/sociala-medier/brist-pa-manliga-influencers-detta-innebar-det-for-marknadsforingen/

Pöyry, E., Pelkonen, M., Naumanen, E., & Laaksonen, S.-M. (2019, August 8). A call for authenticity: Audience responses to social media influencer endorsements in strategic communication. *International Journal of Strategic Communication*, *13*(4), 336–351. https://doi.org/10.1080/1553118 X.2019.1609965

Stoldt, R., Wellman, M., Ekdale, B., & Tully, M. (2019). Professionalizing and profiting: The rise of intermediaries in the social media influencer industry. *Social Media + Society*, *5*(1), 205630511983258. https://doi.org/10.1177/2056305119832587

Tobii Pro. (2022). *Why eye tracking creates value*. Retrieved January 30, 2022, from https://www.tobiipro.com/applications/marketing-user-research/

Winch, A. (2013). *Girlfriends and postfeminist sisterhood*. Palgrave Macmillan. https://doi.org/10.1057/9781137312747

Winch, A. (2015). Brand intimacy, female friendship and digital surveillance networks. *New Formations: A Journal of Culture/Theory/Politics*, *84*, 228–245. https://www.muse.jhu.edu/article/597741

Winship, J. (2000). Survival skills and daydreams. In P. Marris, & S. Thornham (Eds.), *Media studies: A reader* (2nd ed.) (pp. 334–340). New York University Press.

Wood, D. M., & Monahan, T. (2019). Editorial: Platform surveillance. *Surveillance & Society*, *17*(1/2), 1–6. https://doi.org/10.24908/ss.v17i1/2.13237

Wood, S. (2021, June 21). Cannabeauty, lyster och fukt [Cannabeauty, shine and moisture]. *Sofia Wood*. https://sofiawood.elle.se/beauty/cannabeauty-lyster-och-fukt/

Ye, G., Hudders, L., De Jans, S., & De Veirman, M. (2021, March 15). The value of influencer marketing for business: A bibliometric analysis and managerial implications. *Journal of Advertising*, *50*(2), 160–178. https://doi.org/10.1080/00913367.2020.1857888

Zuboff, S. (2015, March 1). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

CHAPTER 4

Tracking (in)fertile bodies

Intimate data in the culture of surveillance

KRISTINA STENSTRÖM
DEPARTMENT OF HUMANITIES, UNIVERSITY OF GÄVLE, SWEDEN

ABSTRACT
Surveillance culture promotes self-improvement through quantified self-knowledge. Digital devices and mobile apps are developed for self-tracking practices, and individuals collect and analyse data about their bodies and habits for numerous purposes. One area of self-tracking involves fertility tracking, through which women track symptoms and signs relating to their menstrual cycle, also called intimate surveillance. Previous research has shown that self-tracking technologies and software often leak data and affect and (re)produce understandings and knowledges of (female) bodies. This chapter explores the following: What are the imaginaries and practices of intimate surveillance among women who use digital apps or wearables to self-monitor their fertility? Through eleven interviews with women who engage in fertility self-tracking, I found multilayered motives and understandings in relation to self-tracking practices, where potential risks are appreciated. Simultaneously, the possibility of fertility self-tracking is seen as a general positive that enables self-knowledge and a sense of empowerment and ownership.

KEYWORDS: intimate surveillance, intimate data, fertility tracking, self-tracking, mobile apps

Stenström, K. (2023). Tracking (in)fertile bodies: Intimate data in the culture of surveillance. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 89–108). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-4

Introduction

An overall focus on self-knowledge and self-surveillance has sparked digital practices where individuals collect information about their bodies and habits through digital devices and software, often referred to as self-tracking or quantifying self. At the same time, an increasing number of mobile apps and digital tracking devices targeting fertility and reproduction are being developed and used for the "intimate surveillance" of subjects and their bodies (Levy, 2019). Technologies such as these are most often designed for women and female bodies, as they generally map menstrual cycles or ovulation or focus on in vitro fertilisation treatments or maternal care. Apps and devices are increasingly connected to artificial intelligence (Johnson, 2014; Lupton, 2016a, 2020; Thomas & Lupton, 2016), which captures and analyses intimate and potentially sensitive data about users, such as ovulation, sexual activity, and medical information (Levy, 2014; Mehrnezhad & Almeida, 2021).

Fertility-tracking apps are often framed and promoted by developers as tools of self-awareness that are more precise and accurate than women's own experiences and interpretations of their bodies and symptoms. The quantification of fertility data is commonly framed as a chance for self-improvement through knowledge that can "impose order on otherwise disorderly or chaotic female bodies" (Lupton, 2015: 446–447), which at times leads users to trust quantifications over their own memories and interpretations (Rettberg, 2018). Users also report that self-tracking and related practices can foster feelings of agency through "a sense of identity, ownership, self-awareness, mindfulness, and control" (Ayobi et al., 2020: 1). Furthermore, data are shareable in social media outlets (Johnson et al., 2019) that may function as "social venues" where self-tracking is discussed (Kent, 2018: 73). Subjects engage in and share self-tracking data as benefits seem obvious, while drawbacks, such as digital trails and commodified and shared data, often remain hidden or abstract.

Drawing on Lyon (2018) and his theorisation of surveillance culture, I explore the imaginaries and practices of intimate surveillance through eleven interviews conducted with women who engage in fertility self-tracking practices. "Intimate self-tracking practices" assemble a variety of actions – such as monitoring bodies and collecting, interpreting, and sharing data – and are facilitated by the combination of human action and technology, such as devices, apps, and their features. Here, imaginaries are theorised through what Charles Taylor and colleagues (2003: 23) have called "social imaginaries", which are defined by the way they are shared by large groups of people, or even entire societies, in a way that legitimises certain practices and understandings as important, true, or even real. Digital (surveillance) practices, which now make up central parts of our social and daily lives, are understood to simultaneously be the product of and produce surveillance culture. Practices and imaginaries are always entangled and intertwined and continuously constitute and reproduce each other. These terms are used here to illustrate how surveillance permeates both individual and collective thought and action on and through multiple levels and facets of the everyday. This chapter explores the following question: What are the imaginaries and practices of intimate surveillance among women who use digital apps or wearables to self-monitor their fertility?

Surveillance culture and self-tracking practices

We are digitally monitored and surveilled in several ways in our everyday lives, and our personal data are harvested for commercial reasons (Zuboff, 2019). While surveillance per se is not a new phenomenon, Lyon (2018: 9) has pointed to a participatory turn in relation to surveillance, where subjects actively engage in the surveillance of others as well as themselves: In novel ways, we comply with but also resist and "even initiate and desire" surveillance. Similarly, Whitaker (1999) has claimed that we are all part of a "participatory Panopticon", as we not only allow but also actively engage in surveillance of ourselves and our habits. Surveillance culture seeps into everyday life in a myriad of ways and is, for instance, manifest in the mundane activities of updating or checking social media channels, where we simultaneously check on others and allow ourselves to be monitored, both by other social media users and by companies that store and share our (meta) data (Marwick, 2012; van Dijck, 2014).

One type of self-surveillance entails the practices of self-tracking, or "lifelogging", where data about habits and bodies are collected, analysed, and shared through digital wearable devices and associated software. The number and variety of mobile apps designed to be used in daily life have grown exponentially during the last decade, not least those designed for self-tracking (Healy, 2021). While individuals have long been tracking personal data – including data relating to fertility – the combination of access to wearable devices and software that can log and process an increasing amount of data has led to a steady rise in the interest in self-tracking (Lupton, 2016a; Rettberg, 2014; Sanders, 2017; Wissinger, 2017).

Dataveillance, which monitors and collects information about subjects "for unstated preset purposes" (van Dijck, 2014: 205), often leaves individuals both unaware and without access to the information collected about them. In contrast, self-tracking presents data to the collecting subjects themselves, who are invited and encouraged to engage in and analyse their own data and its implications (Lupton, 2016b). Lupton (2016b) has noted that self-tracking is becoming increasingly common in contexts where subjects might have little choice regarding participation, such as the workplace, public health, insurance, and so on, and distinguishes between modes of self-tracking that illustrate different levels of voluntariness and independence, ranging from "private self-tracking" to "exploited self-tracking". Private self-tracking is distinguished by being self-initiated and voluntary and undertaken solely for personal reasons and is often connected to motives such as better self-knowledge or the "optimisation of the self". Exploited self-tracking, on the other hand, entails the repurposing of data for commercial reasons to benefit third parties as well as illegal uses of personal data through hacking, for instance.

Digital self-tracking is used in Swedish healthcare for instance regarding childhood obesity (Hagman et al., 2022) and asthma (Ljungberg et al., 2019). This is part of an ongoing investment to implement e-health services in a broader way in Sweden. E-health entails health services that are supported by electronic processes and communication, such as online appointment booking and meetings, as well as the use of self-tracking apps. The government agency Swedish eHealth Agency (2022) is dedicated to issues regarding e-health, and the Swedish government has presented a vision for e-health (Government Offices of Sweden, 2016) to develop such services. Self-tracking is not used routinely in Swedish fertility care but is often initiated by patients themselves before or during fertility treatments (Stenström & Winter, 2021).

Irrespective of whether subjects themselves initiate self-tracking or the practice is suggested by practitioners, there is tension between potential positive and negative outcomes and effects. The literature on self-tracking practices often boils down to questions about whether quantification and ratings stand for empowerment or negative surveillance (Shore & Wright, 2018). Didžiokaitė and colleagues (2018) have pointed to a tendency to understand self-tracking as an "either or" activity, where the Quantified Self–movement and its famous slogan, "self-knowledge through numbers", have been understood as synonymous with self-tracking. The authors claimed that a more nuanced understanding of tracking practices is needed, as numerous users have very moderate goals for their tracking and do not work to "optimise" themselves. Furthermore, everyday users may only use their devices for a short period of time through very basic functions, in contrast to the understandings of avid self-trackers who reinvent their entire outlook on life, and ultimately, *themselves*. Other authors have also identified a need for a more nuanced perspective on self-tracking, as engaged individuals are often not only or primarily on a quest for "objective" numbers or quantified "truths". Kennedy and Hill (2018), for instance, have highlighted that data and their visualisations engage an emotional response among those who produce and take part in them, thus making them more complex and multifaceted than analyses of self-tracking and associated data suggest. Similar to Sharon and Zandbergen (2017), who considered self-tracking as a mode of mindfulness, resistance to social norms and a communicative aid that goes well beyond data-fetishist claims of quantification as a bearer of truth or objectivity, I argue that there is a need to understand and inject nuance into the different meanings that self-trackers attribute to their practices. Thus, in this chapter, I explore how self-trackers navigate the multifaceted understandings that motivate and affect their practices and choices related to intimate self-tracking.

Tracking fertility

As a subgroup to general health-tracking devices and apps, self-tracking also extends to the intimate realms of fertility and sexual life. Several mobile apps used to track menstruation or fertility have been developed. Fertility-tracking apps are part of the wider neoliberal zeitgeist of self-control and self-optimisation, where active engagement in and with fertility and related symptoms is often framed as beneficial, or even necessary, for achieving or avoiding pregnancy or maintaining general health (Ford et al., 2021; Kressbach, 2021). Bodily signs and symptoms that may be tracked include body temperature (which increases after ovulation), mood, energy levels, libido, cramping, vaginal discharge, heaviness and colour of flow, pain, and discomfort. Beyond this, users may also log sexual activity, exercise, intake of alcohol or medications, and so on (Ford et al., 2021; Levy, 2018).

Digital fertility tracking is used to indicate the fertile window in a menstrual cycle, either to avoid or achieve pregnancy (Hamper, 2020). Several fertility-tracking apps offer predictions about potentially fertile days and ovulation days after they have been used for a period of time and users have added enough data for the algorithm to make assumptions about future or past fertility. There are, however, also apps that work more like notepads, as users themselves mark fertile periods based on their bodily symptoms or different fertility awareness methods, where cervix position, discharge, or other symptoms are noted to identify the fertile window of a menstrual cycle. Fertility-tracking apps usually present some form of data visualisation, for instance, graphs, charts, and calendars (Hamper, 2020; Kressbach, 2021). Presenting data as easily reviewable bars and charts contributes to a sense of gamification that motivates users to add more data (Whitson, 2013). Fertility-tracking technologies and associated data are often framed and promoted as "assisting" and "making life easier".

Importantly, however, technology does not innocently measure what is "real" but is both shaped by and shaping the phenomena they are a part of (Johnson, 2020; Lupton, 2018; Wajcman, 2004). Several authors have pointed out that the relationship between humans and technologies maintains and creates understandings, knowledge, and perceptions about fertility and bodies (Andelsman, 2021; Hamper, 2020; Healy, 2021; Lupton, 2018; Stenström & Winter, 2021). Lupton (2018) has also pointed to the "human-data assemblages" in her description of how self-tracking data coproduces understandings and knowledge about human bodies and how humans thus "become with data". Fertility self-tracking creates and maintains understandings, relating to gender in particular, as apps exclusively target women and female bodies.

Fertility-tracking technologies and the collection of fertility data form and affect understandings of fertility and female bodies in several ways. First, as Levy (2019: 687) has claimed, "the act of measurement" legitimises certain forms of knowledge and experiences, while others become invisible. As data are collected and quantified, some sets of data are deemed meaningful and valuable while others are excluded, which in turn coshapes bodies and medical knowledge. Second, apps and tracking (re)produce constructions of femininity and female bodies in other ways. Kressbach (2021), for instance, argued that menstrual- and fertility-tracking apps reinforce discourses of menstrual concealment. In line with a general construction of femininity as free from "abject fluids" or secretions, menstrual- and fertility-tracking apps often use menstrual jokes and euphemisms, which, according to Kressbach, underline menstruation as a taboo subject, as it is concealed linguistically. Healy (2021), on the other hand, claimed that apps and algorithms are designed to compose and present reproductive femininity in particular ways and are thus part of the medicalisation and control of the female body. This type of tracking and quantification can potentially function as continuations of the medical gaze that has been understood to normatively fragment, objectify, and surveil the female body (Balsamo, 1997; Frost & Haas, 2017; Pollack Petchesky, 1987; Seiber, 2016; van der Ploeg, 1995).

Furthermore, much of the information that can be entered into apps tracking menstruation and fertility – and which is needed to make estimations about fertility and fertile periods – can be regarded as especially sensitive and intimate. Much of this data relates to both health and sexual life and can be as detailed as the time of day sex took place or the number of orgasms experienced (Levy, 2019; Shipp & Blasco, 2020), and potentially also relates to intimate life events and issues such as infertility, pregnancy, or abortion (Mehrnezhad & Almeida, 2021). Shipp and Blasco (2020) have found, however, in their review of menstrual-tracking app privacy policies, that app developers frequently fail to consider data about fertility or sex as sensitive. Furthermore, privacy policies are often written in a complicated language and lack the appropriate level of detail, which may obscure how and what data are collected and shared. Healy (2021) argued that due to the increasing commercialisation of fertility data, apps and their terms of use often remain nontransparent regarding how collected data are used and how they might be distributed further to other parties. Data may be stored on commercial platforms and shared with third parties, such as advertisers or employers (Kuntsman et al., 2019; Mehrnezhad & Almeida, 2021; Shipp & Blasco, 2020). Novotny and Hutchinson (2019: 354) noted in their feminist critique of the fertility-tracking app Glow that its "data collection policies erode user agency and, thus, disempower users, the app functions to be supportive of the company rather than its users". They called for a redesign of the app – and others like it – for more transparent practices for gaining access to user health data.

These claims stand in stark contrast to the language of empowerment, self-fulfilment, or self-knowledge often used to promote apps designed to track fertility or menstruation. Ford, De Togni, and Miller (2021) showed in their interview study that women using fertility-tracking apps feel empowered when engaging in "hormonal health" through self-tracking, as this gives them a sense of control over their bodies and emotional lives. However, the authors argued that the very setting that enables and promotes engagement in fertility and hormonal self-tracking is deeply embedded in surveillance capitalism and is, in fact, disempowering in its furtherance of neoliberal self-management. In this chapter, I aim to further explore both the cultural context and the concrete practices associated with fertility self-tracking, which are understood not solely as "positive" or "negative" but bear the potential for both empowerment and exploitation.

Methodological approach

For this study, eleven semistructured interviews were conducted with ten Swedish women and one Finnish woman, who all used different apps and digital technologies to monitor their fertility. Participants were recruited primarily via two Swedish Facebook groups: one focusing on fertility-awareness methods[1] and the other focusing on measures to increase fertility. These groups, which I was somewhat familiar with after doing research for a different study, were chosen and approached as they were expected to include numerous members engaged in fertility self-tracking. Both groups contained frequent posts about fertility tracking, and participants often shared screenshots from their fertility-tracking apps. After approval from group administrators, I published a post where I presented myself and my research interest and requested members interested in being interviewed to contact me. Three interviewees were recruited from my extended network.

Interviewees were between 27 and 38 years old and used one or several of the following mobile apps designed for fertility tracking: Clue, Fertility Friend, Flo, Kindara, Natural Cycles, Premom, and Read Your Body. Interviews were conducted between July 2021 and January 2022 and lasted from 45 minutes to 2 hours each. Due to the Covid-19 pandemic, seven interviews were conducted via digital video-conferencing software, while three were performed in person and one via e-mail. The single e-mail interview was initiated by a participant who preferred to communicate via text. Interview questions focused on how the monitoring and surveillance of bodies is carried out through a combination of digital (apps, etc.) and nondigital (thermometers, ovulation tests, etc.) technologies; what data are collected, where, and with whom they are shared; and how interviewees felt about self-monitoring in regard to privacy. Interviewees were encouraged to take the lead and focus on issues in relation to fertility tracking that they found most important and interesting. Follow-up questions were posed for clarification or for interviewees to expand on particular issues. Most interviewees showed me their apps and typical entries during the interviews or sent me screenshots via e-mail, for me to get a sense of their usage. I also downloaded most apps and familiarised myself with their features.

All interviews were conducted in Swedish, recorded, and subsequently transcribed verbatim for analysis. According to Braun and Clarke (2006: 86), this phase of the research process entails the first phase of analysis as "patterns of meaning and issues of potential interest" are identified during data collection and processed. During the next phase of analysis, I was inspired by a "hybrid approach" to thematic analysis that incorporates data-driven inductive coding and a deductive template of a priori codes (Fereday & Muir-Cochrane, 2006). Whereas the coding of the collected interview material served as the inductive component, the broad categories presented by Lyon (2018) as central to surveillance culture – namely, surveillance practices and surveillance imaginaries – were used for deductive analysis. While Lyon (2018) provided a broader analytical frame to approach surveillance as a cultural and timely phenomenon, inductive coding of the interview material allowed for the identification of further dimensions and facets relating to intimate surveillance, and fertility tracking in particular, to appear.

The coding consisted of first identifying categories as described by Vaismorandi and colleagues (2016), understood as the descriptive and explicit manifestation of the participants' accounts. Transcribed interviews were colour-coded and resulted in the initial codes of 1) self-tracking practices (how, what, when); 2) corporeal self-knowledge (when particular symptoms usually appear and why); 3) emotional self-knowledge (when particular symptoms and emotions usually appear and why); 4) sense of control; 5) sense of agency (identity, ownership, self-awareness, mindfulness); 6) resistance towards standard medical knowledge and methods; 7) resistance towards standard knowledge and suggestions presented by self-tracking apps and technologies; 8) unease or concern about surveillance from developers or third parties; and 9) unease or concern about one's own behaviour (feeling triggered or forced to track, etc.). The coding was done iteratively and recurrently, carefully reading and rereading the material and identifying recurrent ideas and issues therein, as suggested by Vaismorandi and colleagues (2016) and Braun and Clarke (2006). Second, I developed semantic themes and subthemes through interpretation. Third, following Aronson (1995: 2), I developed a "storyline" where "themes that emerge from the informants' stories are pieced together to form a comprehensive picture" of their experiences. Quotes were translated into English for the purposes of this chapter.

Results

I found that the interviewed participants could be divided into two primary groups based on their engagement in established fertility-awareness methods. To my surprise, the engagement in fertility awareness also reflected attitudes towards surveillance issues such as data collection and privacy. The results are presented through four sections. First, I provide a descriptive characterisation of the concrete practices that participants engaged in to surveil themselves and their bodies, for instance, what data were collected and how, but also what apps were chosen and why. The following sections delve deeper into surveillance imaginaries as I present participants' reflections on their engagement and negotiation in matters of (self-) surveillance as a cultural and societal phenomenon.

The collection of "intimate" data

Are surveillance and privacy still appropriate terms to discuss voluntary and active engagement with tracking and checking online, Lyon (2018) asked, or should we understand imaginaries and practices of, for instance, social media or self-tracking in a different light? Furthermore, which data is considered "intimate" – and why – in a time when so much data is collected and shared in different contexts?

All participants in this study engaged in self-tracking their fertility through at least one of the following mobile apps designed for fertility tracking: Clue, Fertility Friend, Flo, Kindara, Natural Cycles, Premom, and Read Your Body. All interviewees used fertility-tracking apps to "get in tune" with their bodies, either to avoid hormonal contraceptives or to better identify their fertile periods in order to achieve or avoid pregnancy and track different indicators of fertility and their general well-being, such as quality of sleep, mood, and exercise. Some participants added information about whether they had consumed alcohol or caffeine.

The choice of app depends partly on the motivation for fertility tracking: An app such as Premom is designed for those planning a pregnancy, and Natural Cycles, for instance, can be set to either support the planning, or the prevention, of pregnancy. Another factor affecting the choice of app or the development of self-tracking practices relates to participants' views on privacy, ownership, and control, as well as self-awareness, both in relation to app developers and their motives and in relation to technology and algorithmic choice and interpretation. Each interviewee expressed awareness of potentially sharing their data both with developers and third parties when engaging in self-tracking through devices and apps, either through intentional harvesting or through data leaks. Participants could, however, be divided into two primary groups that, while sharing several of the concrete self-surveilling practices associated with fertility tracking, were marked by somewhat different motives and perceptions regarding their engagement with fertility tracking and their relationship with data sharing.

The first group was engaged in established fertility awareness methods and characterised by choosing apps that claim to not share data with third parties. This group emphasised their own autonomy and authority in relation to algorithmic interpretations and primarily chose apps such as Read Your Body, which does not present assumptions or interpretations about fertility.

Instead, users “close” and “open” their fertile window in the app based on their physical symptoms. This app is customisable, as the user controls and adds what values and categories should be included, such as temperature or cramping. The second group consisted of individuals who were not trained in fertility awareness but who used fertility apps as a method to either achieve or avoid pregnancy. This group more often chose apps such as Natural Cycles, which is preprogramed to a higher degree and also makes suggestions and interpretations about the fertility status of the user. Thus, there is a difference between the two groups in the way they engage in and affect the “act of measurement” (Levy, 2019), as the first group, to a certain degree, added to and injected nuance into *what* was measured and quantified.

All interviewees except one tracked their body temperature to indicate fertile periods during their cycle, typically using an oral thermometer. One participant who was engaged in fertility awareness measured her vaginal temperature, as she experienced that this gave her the most accurate readings, and thus a clearer and more even statistical curve in her app. When taking the basal body temperature, the most reliable results are achieved by taking readings when waking up and at the same time every morning. Several participants, primarily those engaged in fertility awareness, instead used a “Tempdrop”, which is a device that is placed on the upper arm before going to bed and kept there during sleep. The Tempdrop device does several readings of the body temperature during the night, which can then be transferred to an associated app, or another app, that presents the statistical results. Participants selected this choice because maintaining the habit of waking up at the same time every morning to take their temperature was found to be inconvenient and difficult. The group engaged in fertility awareness also engaged in several additional nondigital practices to surveil their bodies and cycles, such as checking their vaginal discharge or the position of their cervix.

In both groups, several participants logged their sexual activity. A few participants explained that information and data about sex felt more private and intimate than data about their fertility or related symptoms. This is explained by the feeling of sex as something that is clearly chosen, while hormonal shifts and symptoms are something that happens beyond the control of conscious decisions. When sharing her charts with me, one participant removed her entries related to sex, while showing me the rest of her logs.

Several participants from both groups took part in what could be called an extended digital engagement in issues related to fertility self-tracking. This engagement takes place across their fertility apps, social media, and diverse online fora. Some apps, such as Fertility Friend, offer “galleries”, where users can post and share their anonymised charts for others to compare and discuss similarities and differences, for instance, when sharing the same diagnosis or fertility issue. One participant explained that she used this function frequently, but without posting her own charts. In this way, charts from other users – and thus, in a sense, other bodies – became part of the interpretative work this participant did in relation to her own body and fertility. As most of my respondents were part of Facebook groups engaged in fertility awareness or fertility overall, these are also frequently used: Participants read other member's posts and charts or pose questions about both fertility and tracking methods. Some participants also shared their own data, most often in the form of charts.

Thus, what emerged from my interviews was that participants typically shared an interest in surveilling their fertility because they found it helpful for their overall well-being, allowing them to avoid hormone-based contraceptives or identify specific symptoms and their timing (I return to this shortly). Several participants had also invested in additional digital devices specifically to monitor their fertility, such as the Tempdrop device. Most participants' interest in fertility self-surveillance also extended to the practices and results of others or to share their own data with others, thus making corporeal surveillance and interpretation a partly collective endeavour. Thus, the sense of "intimacy" of intimate data related to specific spheres and contexts of identified networks, such as friends or family, or a specific identified individual, such as me, whom they had met face to face. However, "intimate" details in the data could be shared with unidentified others without issue.

Living in and with surveillance culture

> In the end, you kind of surrender, you are surveilled anyways. You kind of only hope for the best. Like, accept all cookies. (Interview with Tina)

Participants clearly reflected on their (self-)surveillance practices as part of a wider cultural tendency. While not referring explicitly to "a culture" of surveillance, participants returned to both the factual circumstances and the sense of being watched and surveilled in close to all their daily practices. Several interviewees expressed concern that they are surveilled and self-surveilled through several everyday practices and devices, such as bank and credit cards, cards for public transportation, a myriad of apps that can track a user's geographical position, shopping habits and patterns, interactions, and so forth:

> I've grown up with Facebook, Instagram, Google, and Gmail. I know they collect data about me and how I use websites. I feel uncomfortable about it, but at the same time it's become an essential condition of our time. It's like, "Okay, this is what you must accept to use these services", that have become the dominant way for us to interact. (Interview with Anja)

Participants expressed clear awareness of their own surveillance practices, and their place in a surveillance culture overall, by acknowledging that their whereabouts and data are likely collected and stored. While participants do experience some issues relating to the continuous surveillance of their daily habits and lives as worrisome or unpleasant, all of them still expressed a level of acceptance of this order and societal reality. In terms of imaginaries, participants conceived of surveillance as a societal necessity and expressed that there were no ways of functioning properly in a society that relied so heavily on the collection of data and information without complying with that way of living and acting. Thus, participants identified compliance and understanding regarding surveillance, both on an individual and a societal level, which indicates a (social) imaginary of surveillance as unavoidable but also as necessary and beneficial in certain respects. At the same time, however, another competing societal narrative raises critiques and concerns regarding digital surveillance. Trying to accomplish an existence free from – or even with a reduced amount of – shared information and data would be like trying to turn back time. As this is impossible, the right thing, instead, is to stay informed and alert and to harvest the positive effects of surveillance:

> With all technology, it's in the back of your mind, who can get hold of this information? However, still, I just think, this is the way we must live now. In addition, I feel like, if someone wants to analyse my data – well, go ahead! The positives outweigh the negatives. (Interview with Maja)

Participants expressed some concern about the risk of their fertility data and its links to intimate life events, such as pregnancies (Mehrnezhad & Almeida, 2021), leaking or winding up in unforeseen or unintended contexts. However, several participants expressed that they felt more comfortable with the idea of their data ending up as part of a faceless collection of data "somewhere", while they might not want to share their data even with friends. Some participants also expressed that they wished for their data to be used for research on women's health and other "collective good" purposes. Generally, interviewees were more focused on the risk of their data or information ending up among their identified networks, namely, among people they know and who know them. This also extends to Facebook groups and other identified social media, where participants were willing to share intimate details with strangers while being restrictive about even posting everyday updates within their networks of "friends". Thus, privacy is divided into spheres, where the most important sphere is among identified "real life" contacts, among whom respondents may be very restrictive with information sharing. As stated above, the "intimacy" of intimate data presupposes identified networks, and the sense of intimacy regarding data subsides to a degree when data are collected by "faceless" third parties.

Taking control and being empowered

> It would be fair to share how the body works and then leave it to everyone to make up their minds about what protection to use. It's absurd that it all falls on women. Not only when you have a partner, but always. What if someone wants to sleep with you? You better be ready! Because, once a month I have an egg, and all these men walk around with their sperm all the time. (Interview with Tina)

All participants who engaged in self-tracking of their fertility expressed that they have learned a lot about their bodies. Nearly all participants raised concerns over the fact that girls and women are routinely offered hormonal contraceptives rather than counselling and information about how their fertility actually works. Participants linked this to an overall patriarchal view of women and their bodies, where women are often expected to take sole responsibility for family planning and contraceptives, while simultaneously not having the choice to decide for themselves about the best option for their hormonal health. Routine information that is distributed to women (and men), according to participants, is based on an average menstrual cycle of 28 days, where ovulation occurs on the fourteenth day of the cycle. This, however, is far from reality for everyone, as there are considerable differences between women, which is largely ignored in the information given in schools, by physicians, and through the overall societal narrative about female fertility.

Several participants who engaged in fertility awareness also expressed that several apps developed for fertility tracking reproduced and cemented inaccurate or dated knowledge about fertility or menstrual cycles, in line with the findings of Andelsman (2021), Hamper (2020), and Healy (2021). Additionally, they felt that fertility apps would sometimes not truly inform users about how and why certain interpretations about fertile periods were done, but only presented estimations. This, in turn, led to users remaining dependent on apps while not learning about their own fertility.

All participants attributed a sense of agency and empowerment to their self-surveillance practices in relation to fertility. However, those participants who were engaged in established fertility awareness methods found these methods to be the most meaningful and important features in developing self-awareness and a sense of control and empowerment in relation to their own bodies and fertility. The group of participants who were not engaged in fertility awareness and who used "mainstream" apps, on the other hand, felt that app use in itself was greatly helpful in introducing them to new knowledge and adding to their self-awareness. This was made possible through features such as information texts and through insights participants gained through app use, as they added information and identified patterns and recurrent symptoms through the overview the app offered:

> The apps, fertility awareness overall, feel slightly like concurring yourself. Even if you can't control everything, you still feel like you have an understanding… control the understanding of yourself. (Interview with Nina)

The sense of being empowered was also linked to and negotiated through the use of self-tracking technologies and apps. Where close to all participants expressed concern about patriarchal attitudes and lack of knowledge about female bodies and fertility, the fear or concern about the loss of ownership and control extended to the use of self-tracking technologies, primarily among those participants who engaged in fertility awareness methods. These participants also expressed an attitude, as well as attempts, to achieve and maintain a sense of independence, and thus empowerment, towards self-tracking technology and apps themselves. Those participants who were most actively engaged in fertility awareness also expressed a more deep reliance on their own interpretations of their physical symptoms, and they gave tracking apps and devices less room to influence their interpretations and assumptions about their fertility, physical state, or overall health. For them, resisting or negotiating the interpretations presented by algorithms and predefined categories was simultaneously a way to resist and negotiate dominant medical narratives or "knowledge" about female corporeality.

The other group of participants who were not actively engaged or knowledgeable about fertility awareness did not express the same scepticism regarding interpretations or suggestions made by technological devices and apps that they used. They instead focused their concern on how their data might be handled and found self-tracking devices, associated software, and algorithms to mostly be helpful in interpreting bodily signs and symptoms. Here, participants' own bodies and their understanding of their own symptoms come together with and illustrate a wider social imaginary of self-optimisation and self-knowledge. This is done in part through a celebratory understanding of technological opportunities. However, the corporeal is also understood as a potential site of resistance, as its true knowledge of bodily symptoms is understood to crystallise the limitations of technological ability, which cannot trump self-knowledge.

Optimisation and gamification

In line with identifying (self-)surveillance practices as part of a wider zeitgeist, participants also reflected on how fertility tracking was part of an overall focus on performance and (self-)control. One participant identified a false sense of control, where she would feel a momentary relief and sense of taking charge when entering her data into an app or seeing "a nice graph" created by the application based on her measurements and data. This echoes the results of Ford and colleagues (2021), who underlined the paradox between a sense of empowerment and control in the context of neoliberal self-management that demands continuous self-improvement and endless "work" to maintain that sense. The participant simultaneously acknowledged that her careful and precise data collection had no impact whatsoever on her hormones or symptoms related to hormonal health:

> It's truly good but triggering at the same time. You feel like you end up in a kind of accomplishment. (Interview with Nina)

Both this participant and others identified that they at times were affected by a sense of force or obsession that they were uncomfortable with, by checking or comparing their charts "too often" or becoming "too" preoccupied with adding or excluding factors in their daily lives to optimise their hormonal health and, through that, their fertility and overall well-being. In these statements, participants identified the discourses of self-improvement as central to "the project of the self" and how those discourses affect and alter their behaviour and state of mind. Relatedly, several participants identified the gamification features of the apps as an active part of their periodical self-identified "obsession" with entering and interpreting data. According to Whitson (2013), gamification is often a part of surveillance, as it motivates subjects to willingly share their information through the pleasurable experience of play. Participants experienced this in the sense that their apps presented "beautiful charts" or congratulated them on a job well done. Several participants had taken breaks from self-monitoring their fertility to free themselves from the pressures and demands they experienced in relation to continuous monitoring. However, all of them subsequently returned to self-monitoring their fertility markers.

Conclusion

This chapter has explored the practices and imaginaries of intimate surveillance of women who engage in fertility self-tracking. The analysis was driven by the exploration of what and how women who engage in self-tracking their fertility go about their surveillance practices and how their imaginaries of surveillance and surveillance culture both motivate their practices and contribute to the reproduction of the cultural momentum of surveillance. Following Taylor and colleagues (2003), social imaginaries are understood as comprehension and agreement about societal conditions and legitimate actions that reach beyond individuals and are shared by a wider public. However, in this chapter, imaginaries also refer to individual motives, understandings, and concerns, which are intimately associated with (both produced by and productive of) wider social imaginaries.

In line with previous studies (Kennedy & Hill, 2018; Sharon & Zandbergen, 2017), I would like to draw attention to how individuals engaged in self-tracking have multilayered motives and understandings of their practices, in which they often understand and appreciate potential risks, but where the effects or consequences rendered as meaningful or helpful are regarded as more important. While participants are critical and, in some cases, concerned, in most cases, they view the tracking and potential sharing of fertility data as something that is to be expected in a time and culture that relies so heavily on data collection and storage. By choosing between potential negatives and positives, participants argued that they feel they have little room to change or affect the way current societal structures revolve around information collection. Instead, they wished to benefit from the opportunities and positive aspects of this cultural moment that also offers them tools to collect and interpret data and information in an unprecedented way.

What especially connects the themes that came forth during the analysis is the sense of control that participants expressed having or seeking, primarily associated with access to information and the capacity and confidence to make interpretations. The sense of control or ownership that participants rendered important was not primarily about avoiding surveillance or the commodification of their data, but about knowing and understanding the scope of surveillance. Participants also took different measures to balance their relationship to self-tracking, such as taking time off from tracking, as associated risks are identified not only in relation to app developers or third parties, but also in relation to the well-being of participants themselves. For instance, participants sometimes experienced that tracking practices become forced or are accompanied by a sense of constraint.

On the note of ownership and control, several participants also stressed the importance of making their own interpretations of the collected data. While they used apps to collect, and sometimes analyse, data, several participants emphasised their own interpretations as primary. In part, this relates to a sentiment that several participants shared: Living, breathing humans are best equipped to read and interpret their own bodies. The sense of remaining critical towards devices, apps, and associated algorithms also extends to resisting a perceived "one size fits all" in relation to female corporeality and fertility, where self-tracking technologies both reflect and reproduce specific normative bodies.

The results of this study are, of course, dependent on the selection and distribution of participants. As this study targeted persons using fertility tracking, all involved participants were engaged in this practice. Had individuals who for some reason had chosen not to engage in digital fertility tracking been included, the results would have been different. While those most sceptical of collecting and sharing data about their fertility also likely refrained from doing so, my experience from the interviews was that participants made conscious decisions about their fertility tracking. They did not share a solely celebratory or naïve view of data collection but found that the positives outweigh the negatives.

Acknowledgements

I would like to thank the interviewees who generously shared their experiences with fertility tracking. Interviewees also provided important nuances through their insights and perspectives that improved the study in a significant way.

References

Andelsman, V. (2021). Materializing: Period-tracking with apps and the (re) constitution of menstrual cycles. *MedieKultur: Journal of Media and Communication Research, 37*(71), 54–72. https://doi.org/10.7146/mediekultur.v37i71.122621

Aronson, J. (1995). A pragmatic view of thematic analysis. *The Qualitative Report*, *2*(1), 1–3. https://doi.org/10.46743/2160-3715/1995.2069

Ayobi, A., Marshall, P., & Cox, A. L. (2020, April). Trackly: A customisable and pictorial self-tracking app to support agency in multiple sclerosis self-care. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–15). https://doi.org/10.1145/3313831.3376809

Balsamo, A. (1997). *Technologies of the gendered body: Reading cyborg women*. Duke University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Didžiokaitė, G., Saukko, P., & Greiffenhagen, C. (2018). The mundane experience of everyday calorie trackers: Beyond the metaphor of Quantified Self. *New Media & Society*, *20*(4), 1470–1487. https://doi.org/10.1177/1461444817698478

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92. https://doi.org/10.1177/160940690600500107

Ford, A., De Togni, G., & Miller, L. (2021). Hormonal health: Period tracking apps, wellness, and self-management in the era of surveillance capitalism. *Engaging Science, Technology, and Society*, *7*(1), 48–66. https://doi.org/10.17351/ests2021.655

Frank-Herrmann, P., Heil, J., Gnoth, C., Toledo, E., Baur, S., Pyper, C., Jenetzky, E., Strowitzki, T., & Freundl, G. (2007). The effectiveness of a fertility awareness based method to avoid pregnancy in relation to a couple's sexual behaviour during the fertile time: a prospective longitudinal study. *Human Reproduction*, *22*(5), 1310–1319. https://doi.org/10.1093/humrep/dem003

Frost, E., & Haas, A. M. (2017). Seeing and knowing the womb: A technofeminist reframing of fetal ultrasound toward a decolonization of our bodies. *Computers and Composition*, *43*, 88–105. https://doi.org/10.1016/j.compcom.2016.11.004

Government Offices of Sweden. (2016). *Vision for eHealth 2025 – common starting points for digitisation of social services and health care*. Ministry of Health and Social Affairs. https://ehalsa2025.se/wp-content/uploads/2021/02/vision-for-ehealth-2025.pdf

Hagman, E., Johansson, L., Kollin, C., Marcus, E., Drangel, A., Marcus, L., Marcus, C. & Danielsson, P. (2022). Effect of an interactive mobile health support system and daily weight measurements for pediatric obesity treatment, a 1-year pragmatical clinical trial. *International Journal of Obesity*, *46*, 1527–1533. https://doi.org/10.1038/s41366-022-01146-8

Hamper, J. (2020). 'Catching ovulation': Exploring women's use of fertility tracking apps as a reproductive technology. *Body & Society*, *26*(3), 3–30. https://doi.org/10.1177/1357034X19898259

Healy, R. L. (2021). Zuckerberg, get out of my uterus! An examination of fertility apps, data-sharing and remaking the female body as a digitalized reproductive subject. *Journal of Gender Studies*, *30*(4), 406–416. https://doi.org/10.1080/09589236.2020.1845628

Johnson, B., Quinlan, M., & Pope, N. (2019). #ttc on Instagram: A multimodal discourse analysis of the treatment experience of patients pursuing in vitro fertilization. *Qualitative Research in Medicine and Healthcare*, *3*(1), 1–14. https://doi.org/10.4081/qrmh.2019.7875

Johnson, E. (2020). *Refracting through technologies: Bodies, medical technologies and norms*. Routledge. https://doi.org/10.4324/9781315122274

Johnson, S.A. (2014). "Maternal devices", social media and the self-management of pregnancy, mothering and child health. *Societies*, *4*(2), 330–350. https://doi.org/10.3390/soc4020330

Kennedy, H., & Hill, R. L. (2018). The feeling of numbers: Emotions in everyday engagements with data and their visualisation. *Sociology*, *52*(4), 830–848. https://doi.org/10.1177/0038038516674675

Kent, R. (2018). Social media and self-tracking: Representing the 'health self'. In B. Ajana (Ed.), *Self-tracking: Empirical and philosophical investigations* (pp. 61–76). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65379-2

Kressbach, M. (2021). Period hacks: Menstruating in the big data paradigm. *Television & New Media*, *22*(3), 241–261. https://doi.org/10.1177/1527476419886389

Kuntsman, A., Miyake, E., & Martin, S. (2019). Re-thinking digital health: Data, appisation and the (im)possibility of 'opting out'. *Digital health*, *5*, 2055207619880671. https://doi.org/10.1177/2055207619880671

Levy, J. (2018). Of mobiles and menses: Researching period tracking apps and issues of response-ability. *Studies on Home and Community Science*, *11*(2), 108–115. https://doi.org/10.1080/09737189.2017.1420400

Levy, K. E. C. (2019). Intimate surveillance. *Idaho Law Review*, *51*(3), 679–693. https://digitalcommons.law.uidaho.edu/idaho-law-review/vol51/iss3/5

Ljungberg, H., Carleborg, A., Gerber, H., Öfverström, C., Wolodarski, J., Menshi, F., Engdahl, M., Eduards, M., & Nordlund, B. (2019). Clinical effect on uncontrolled asthma using a novel digital automated self-management solution: A physician-blinded randomised controlled crossover trial. *European Respiratory Journal*, *54*(5), 1900983. https://doi.org/10.1183/13993003.00983-2019

Lupton, D. (2015). Quantified sex: A critical analysis of sexual and reproductive self-tracking using apps. *Culture, health & sexuality*, *17*(4), 440–453. https://doi.org/10.1080/13691058.2014.920528

Lupton, D. (2016a). Mastering your fertility: The digitised reproductive citizen. In A. McCosker, S. Vivienne, & A. Johns (Eds.), *Negotiating digital citizenship: Control, contest and culture* (pp. 81–93). Rowman & Littlefield.

Lupton, D. (2016b). The diverse domains of quantified selves: Self-tracking modes and dataveillance. *Economy and Society*, *45*(1), 101–122. https://doi.org/10.1080/03085147.2016.1143726

Lupton, D. (2018). How do data come to matter? Living and becoming with personal data. *Big Data & Society*, *5*(2), 2053951718786314. https://doi.org/10.1177/2053951718786314

Lupton, D. (2020). Caring dataveillance: Women's use of apps to monitor pregnancy and children. In L. Green, D. Holloway, K. Stevenson, T. Leaver, & L. Haddon (Eds.), *The Routledge companion to digital media and children* (pp. 393–402). Routledge. https://doi.org/10.4324/9781351004107-37

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

Marwick, A. (2012). The public domain: Surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Mehrnezhad, M., & Almeida, T. (2021, May). Caring for intimate data in fertility technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (pp. 1–11). https://doi.org/10.1145/3411764.3445132

Novotny, M., & Hutchinson, L. (2019). Data our bodies tell: towards critical feminist action in fertility and period tracking applications. *Technical Communication Quarterly*, *28*(4), 332–360. https://doi.org/10.1080/10572252.2019.1607907

Pollack Petchesky, R. (1987). Fetal images: The power of visual culture in the politics of reproduction. *Feminist Studies*, *13*(2), 263–292. https://doi.org/10.2307/3177802

Rettberg, J. W. (2014). *Seeing ourselves through technology: How we use selfies, blogs and wearable devices to see and shape ourselves*. Palgrave Macmillan. https://doi.org/10.1057/9781137476661

Rettberg, J. W. (2018). Apps as companions: How quantified self apps become our audience and our companions. In B. Ajana (Ed.), *Self-tracking: Empirical and philosophical investigations*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65379-2

Sanders, R. (2017). Self-tracking in the digital era: Biopower, patriarchy, and the new biometric body projects. *Body & Society*, *23*(1), 36–63. https://doi.org/10.1177/1357034X16660366

Seiber, T. (2016). Ideal positions: 3D sonography, medical visuality, popular culture. *Journal of Medical Humanities*, *17*(1), 19–34. https://doi.org/10.1007/s10912-015-9350-8

Sharon, T., & Zandbergen, D. (2017). From data fetishism to quantifying selves: Self-tracking practices and the other values of data. *New Media & Society*, *19*(11), 1695–1709. https://doi.org/10.1177/1461444816636090

Shipp, L., & Blasco, J. (2020). How private is your period? A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies*, *2020*(4), 491–510. https://doi.org/10.2478/popets-2020-0083

Shore, C., & Wright, S. (2018). Performance management and the audited self. In B. Ajana (Ed.), *Metric culture: Ontologies of self-tracking practices*. Emerald. https://doi.org/10.1108/978-1-78743-289-520181002

Stenström, K., & Winter, K. (2021). Collective, unruly, and becoming: Bodies in and through ttc-communication. *MedieKultur: Journal of Media and Communication Research*, *71*(31–53). https://doi.org/10.7146/mediekultur.v37i71.122653

Swedish eHealth Agency. (2022). *Welcome to the Swedish eHealth agency*. https://www.ehalsomyndigheten.se/languages/english/welcome-to-the-swedish-ehealth-agency/

Taylor, C., Gaonkar, D. P., Kramer, J., Lee, B., & Warner, M. (2003). *Modern social imaginaries*. Duke University Press. https://doi.org/10.1515/9780822385806

Thomas, G. M., & Lupton, D. (2016). Threats and thrills: Pregnancy apps, risk and consumption. *Health, Risk & Society*, *17*(7-8), 495–509. https://doi.org/10.1080/13698575.2015.1127333

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice*, *6*(5), 100–110. http://dx.doi.org/10.5430/jnep.v6n5p100

van der Ploeg, I. (1995). Hermaphrodite patients: In vitro fertilization and the transformation of male infertility. *Science, Technology, & Human Values*, *20*(4), 460–481. https://www.jstor.org/stable/689870

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Wajcman, J. (2004). *TechnoFeminism*. Polity Press.

Whitaker, R. (1999). *The end of privacy: How total surveillance is becoming a reality*. The New Press.

Whitson, J. R. (2013). Gaming the quantified self. *Surveillance & Society*, *11*(1/2), 163–176. https://doi.org/10.24908/ss.v11i1/2.4454

Wissinger, E. (2017). Wearable tech, bodies, and gender. *Sociology Compass*, *11*(11), e12514. https://doi.org/10.1111/soc4.12514

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

Endnotes

[1] Fertility awareness–based methods include family-planning methods that are based on the woman's observation of signs and symptoms of fertile and infertile periods, either to achieve or to avoid pregnancy. Fertility-awareness methods depend on both the accurate identification of fertile days and the modification of sexual behaviour to either achieve or avoid pregnancy (Frank-Herrmann et al., 2007).

CHAPTER 5

It all depends on context

Danes' attitudes towards surveillance

RIKKE FRANK JØRGENSEN
THE DANISH INSTITUTE FOR HUMAN RIGHTS, DENMARK

ABSTRACT
It is often emphasised that Danes are relatively tolerant to state surveillance, and seen from a European perspective, there is a high degree of trust between citizens and the state in Denmark. The question is, however, where Danes set the boundaries for different types of state surveillance. Based on findings from the Danish Values Survey, this chapter analyses Danish citizens' views on three categories of state surveillance: CCTV surveillance in public places; monitoring of e-mails and other information exchanged on the Internet; and the collection of information on citizens without their knowledge. It argues that the considerable variations in the Danes' attitudes towards the three types of surveillance may be explained by the different types of exposure they entail, as well as the privacy norms associated with each.

KEYWORDS: Danes, attitudes towards surveillance, state surveillance, CCTV, privacy norms

Jørgensen, R. F. (2023). It all depends on the context: Danes' attitudes towards surveillance. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 109–124). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-5

Introduction

In recent years, there has been an increasing debate on the normalisation of surveillance (Wood & Webster, 2009) and about surveillance as a necessary (and often useful) part of Denmark's welfare state (Lauritsen, 2021). Likewise, the Orwellian state-centric concept of surveillance is challenged by the digital age of smartphones, social media, intelligent sensors, Big Data, and so on. Surveillance is no longer just something the state subjects its citizens to, but something we ourselves are a part of (Harcourt, 2017; see also Stenström, Chapter 4). Information is shared voluntarily and involuntarily on digital platforms, and people monitor themselves with technologies and services as part of exercising, sleeping, and eating, for example. In other words, we live in a culture of surveillance (Lyon, 2018). In response to this surveillance culture, the right to privacy – as well as data protection – is often emphasised as a norm that delimits surveillance, especially within Europe. However, there are several shortcomings to the privacy argument, including the lack of a common definition (and understanding) of privacy and its individual and societal value (Koops et al., 2017; Solove, 2008; see also Kaplan, Chapter 2).

In a welfare state such as Denmark, the state's collection and processing of information about its citizens – from birth to death – is an integral part of the welfare model, and something most citizens accept as a given social premise. Compared with other European countries, there is a high degree of trust between citizens and the state in Denmark (Frederiksen, 2019a). The question is, however, where Danes set the boundaries for different types of state surveillance.

Against the backdrop of the Danish Values Survey (Frederiksen, 2019b), this chapter analyses the Danes' views on surveillance. The survey asked the respondents about their willingness to let the state conduct surveillance in three different situations: 1) CCTV surveillance in public places; 2) monitoring of e-mails and other information exchanged on the Internet; and 3) the collection of information about Danes without their knowledge. Based on the survey results, it examines the differences in attitudes towards the three types of surveillance, as well as the characteristics of those who are most positive or most critical towards surveillance, for example, the connection between age and attitudes towards surveillance; between political affiliation and attitudes to surveillance; and between the attitude to terror, trust in people of another nationality, and to surveillance.[1]

On a theoretical basis, the chapter draws on surveillance literature (Bogard, 2006; Harcourt, 2017; Lyon, 2018) and begin by exploring the notion of surveillance and how it relates to a digital welfare state such as Denmark. In building the theoretical framework, it draws upon the notion of exposure (Ball, 2009), the surveillance characteristic (Marx, 2006), and the privacy expectations associated with a specific context (Nissenbaum, 2010). In the next, and more empirical, part, these notions are used to understand and explain the considerate variations in the Danes' attitudes towards surveillance across the three types of surveillance addressed in this chapter. It suggests that the general support for CCTV surveillance and the relative lack of support for the other two categories of surveillance may be explained by the kind of surveillance measure proposed, the type of exposure they entail, as well as the privacy expectations related to the context they target.

The notion of surveillance and its shortcomings

Surveillance is a topic embedded with socio-technical questions about power, data, and control. The term surveillance has historically been related to the authorities' means of watching citizens, for example, in prisons and places of confinement, as part of law enforcement and intelligence practices, and a general means to detect wrongdoings in society (Haggerty & Ericson, 2006; Marklund, 2020). Marklund (2020) situated the birth of mass surveillance at the start of World War I in 1914, when Britain led the development of a government-backed regime for mass surveillance of electric and postal communications across Europe.

Over the past 20 years, there has been a shift in surveillance discourse and practices, leading to a normalisation of surveillance. In the aftermath of the terrorist attacks on the World Trade Center on 11 September 2001, the scope of surveillance measures increased significantly in most parts of the world (Lyon, 2003). Likewise, it became a significant element in the discourses on anti-terrorism and public security, which provided surveillance practices with some level of legitimacy. Fast forward to today, and surveillance has become a general practice used by both public and private institutions, including for several citizen-serving purposes, such as supporting elderly persons in their own homes or monitoring people with severe diseases. Moreover, surveillance is built into the fabric of social media and smart technology, and thus into everyday life (Harcourt, 2017). As such, surveillance practices have shifted from centralised to more "smooth" forms of observation. Technological developments have been key in the rise of new forms of surveillance, from automation and control (Agre, 1994; Beniger, 1986) to the type of ubiquitous surveillance that characterise the "smart" digital society (Harcourt, 2017; Zuboff, 2019). With their concept of surveillance assemblage, Haggerty and Ericson (2006) contemplated the disconnected character of contemporary surveillance practices and argued that part of modern surveillance power comes from the ability to combine and draw upon different data systems, which may then be used to serve various purposes.

Given the broad category of practices that contemporary surveillance encompasses, one might consider whether the notion remains useful for examining such diverse societal and technological practices in a meaningful way. Moreover, surveillance is normatively charged and does not distinguish between a states' legitimate data collection and control and the illegitimate surveillance of citizens that is often associated with the term. The legitimacy of surveillance may change depending on the situation, purpose, and use of the data; therefore, it may provide more clarity to differentiate between legitimate and illegitimate practices whereby someone acquires knowledge about someone else, rather than use surveillance as a universal term, often with the connotation of the misuse of power. In the public debate on surveillance in Denmark, for example, the term often serves to polarise rather than to qualify the concrete practices at stake and why they may be problematic.[2]

Another shortcoming related to surveillance discourses concerns the lack of an individual perspective. Whereas surveillance studies have had a strong focus on the exercise of power and control, they have been less occupied with the individual implications of surveillance, including how people understand and make sense of surveillance measures. Ball (2009) stressed that surveillance practices have consequences for the individual and proposed the concept of exposure to describe the individual experience of surveillance. A key point in relation to exposure is the surveilled subject being more open to classification and scrutiny, since there is now a political economy of "interiority", or "a process where an aspect of an individual's personal or private world becomes exposed to others, via a process of data representation, interpretation, sharing" (Ball, 2009: 643). Since both the public and private sectors process and repurpose large amounts of data representing different aspects of people's lives, those with access to data hold the key to defining the characteristics around which people will be sorted and targeted as part of this exposure economy. We return to the notion of exposure when examining the results from the Danish Values Survey.

The assessment of surveillance practices

The surveillance resistance literature (Gilliom, 2006) provides insight into public attitudes towards surveillance. An important point from this line of work is the need to recognise that surveillance is experienced differently depending on the specific circumstances of a person's situation (Gilliom, 2006). Public responses to surveillance initiatives vary greatly across countries and regions, from no response to public demonstrations and campaigns, petitions, litigations, gaming the system, or using technical means such as encryption. Likewise, it depends on the concrete situation and surveillance measure deployed.

The privacy discourse has often been positioned as a counter-narrative to surveillance; however, the strength of the privacy argument is contested (Cohen, 2013; Haggerty & Ericson, 2006), just as the ever-growing body of privacy literature lacks a common understanding of what privacy entails, and why it is important. Within the European Union, the individual's right to the respect of privacy and data protection is stipulated in the EUs Charter of Fundamental Rights (EU Parliament, 2000) and the European Convention of

Human Rights (Council of Europe, 1950). According to these legal norms, the right to privacy is not unlimited, but any restriction to the right – such as state surveillance – must follow the criteria laid out in Article 8 of the European Convention of Human Rights: have a legal basis, serve a legitimate aim, and be necessary and proportionate to that aim. The European Union also has the world's most expansive data protection regulation (GDPR), covering privacy and data protection within both public and private institutions; however, this legal framework cannot fully address the challenges of the data-driven economy, including tech giants (Vanberg, 2021; Hoboken, 2019).

In her substantive contribution to the privacy discourse, Nissenbaum argued with her theory of contextual integrity that privacy concerns largely depend on context:

> A right to privacy is neither a right to secrecy nor a right to control but a right to *appropriate flow* of personal information [...] but what this (privacy) amounts to is a right to contextual integrity and what *this* amounts to varies from context to context [emphasis original]. (Nissenbaum, 2010: 127).

According to the theory of contextual integrity, privacy is preserved when information flows about an individual conform to legitimate contextual informational norms. Likewise, privacy is breached when contextual informational norms are not adhered to. While pointing to the important role of context, the theory seems to presume that contexts are relatively delimited spaces with "contextual information norms" that can be established. In practice, however, establishing the appropriate contextual norms for any given "information flow" is not a straightforward exercise, especially in relation to digital services and networks that have no predecessors in the physical world, and thus lack a clear normative point of reference. For example, a context like a social media site may entail several different, or even conflicting, contextual norms.

Leaning on the European approach to privacy and data protection, Marx (2006) has proposed that the normative assessment of surveillance may be based on the following five factors: 1) the characteristic of the surveillance means used (e.g., its level of bodily invasiveness, its degree of openness vs. covertness, and its level of validity); 2) the application of the measure, including its data collection and processing (thus, European data protection principles would apply here); 3) the nature and legitimacy of the purpose for surveillance; 4) the structure of the setting in which the surveillance is used (e.g., reciprocal versus non-reciprocal; and 5) the kind of data that is gathered. Such an analysis of the concrete means and criteria for information gathering would also be the starting point in a privacy assessment of surveillance based on the European Convention of Human Rights. In practice, such an assessment would evaluate whether there is a clear and foreseeable law stipulating the surveillance measure, whether it serves a legitimate aim in a democratic society, and whether it constitutes a necessary (and proportionate) measure to that aim. If these criteria are not met, the surveillance measure would be in violation of the individual's right to privacy (European Court of Human Rights, 2021).

We return to the character of the surveillance measure (Marx, 2006), Nissenbaum's privacy expectations (2010), and the notion of exposure (Ball, 2009) when analysing the Danes' attitudes towards the three surveillance types.

Denmark as a digital welfare state[3]

Denmark is often presented as a frontrunner in digitalisation,[4] with a highly digitalised public sector and widespread use of technology throughout the population. Over the past 25 years, the government has deployed technology to facilitate public administration and services across a broad range of areas, such as case-handling systems, public (self-)services, childcare and school platforms, healthcare systems, and so on. Moreover, Denmark has a well-developed digital infrastructure in terms of networks and broadband, a mandatory mailbox dedicated to communication between citizens and public authorities, and a digital identification solution (MitID). The high level of digitalisation combined with a unique identification of citizens provides the state with expansive means of controlling as well as serving its citizens. In Denmark, the state's collection of personal information from birth to death is an integral part of the Danish welfare model and is accompanied by a relative high level of trust between citizens and the state. According to Statistics Denmark (2019), for example, a total of 76 per cent of Danes have confidence in how the public authorities manage their personal information. The high level of trust amongst Danes is also distinctive when compared with other European countries (Frederiksen, 2019b). The increasing digitalisation is not unique to Denmark, however, being reflected in the other Nordic countries as well (Buhl, 2022).

Schou and Hjelholt (2019) have studied Danish digitisation strategies from 2002 to 2015 and have pointed to digital citizenship as a key political figure that has been promoted in Danish digitisation strategies through discursive, legal, and institutional means. As part of digital citizenship, Danish citizens are increasingly expected to perform digitally, for example, in relation to public services and social benefits. Likewise, the public administration relies heavily on the processing of vast quantities of data about the individual and uses such data to identify specific areas of intervention, for example, to detect fraud or allocate social benefits, as part of its decision-making processes (Jørgensen, 2021).

In such a data-driven welfare society, surveillance takes on new meaning. Extensive modes of data extraction and data analytics characterise not only tech giants that excel in profiling, predicting, and influencing individuals (Zuboff, 2019), but also provides the public sector with new means of surveillance. When the state controls unprecedented "granular, immediate, varied, and detailed data" about its citizens (Bigo et al., 2019: 3), it effectively has access to extraordinary means of surveillance. In 2019, the UN Special Rapporteur on Extreme Poverty, Philip Alston, warned that "systems of social protection and assistance are increasingly driven by digital data and technologies that are used to automate, predict, identify, surveil, detect, target and punish" (Alston, 2019: 2). Likewise, Kaun and Dencik (2020) pointed to the advent of a new regime of control in public services and welfare provision intricately linked to increased digitalisation, including new risks related to public accountability. The concentration of data about individuals in the hands of the state (and the market) presents knowledge asymmetries and introduces new axes of social inequality in terms of who knows what (Eubanks, 2018). Such asymmetry in access to data, combined with the means to exercise power, calls for scrutiny as to how and for what purpose data is collected, for instance, the extent to which it is used to conduct surveillance and expose irregularities in relation to citizens (Alston, 2019; Eubanks, 2018). At the same time, the nature of the data and how it is collected, combined, and shared is rarely visible to the individual. Moreover, with the advent of artificial intelligence being used to automate decision-making in the public sector, this asymmetry between state and citizens may be accentuated even further.

It is against this background that the Danish Values Survey examined the Danes' attitudes towards state-based surveillance.

The Danish survey: How Danes feel about surveillance

The mapping of Danes' values has been carried out since 1981 as part of a major European Union study. In 2017, three questions related to surveillance were introduced for the first time:

> Do you think that the Danish state should have the right to conduct the following: a) CCTV surveillance of people in public places? b) Surveillance of all emails and other information exchanged on the Internet? c) Gather information about everyone living in Denmark, without their knowledge?

For each question, the respondents could choose between the following four categories of answers: [the state, authors insertion] "should certainly have this right"," should probably have this right", "should probably not have this right", and "should certainly not have this right". The data was collected via interviews and online questionnaires and represents a total of 3,362 responses. The response rate was 50 per cent for the online questionnaire interviews and 42 per cent for the interviews. The data was subsequently analysed based on cross-tables and regression analysis.[5]

The survey reveals that the respondents were generally more positive towards surveillance when responding online compared to when they were being interviewed. There was also a tendency for online respondents to have made less use of the most extreme response categories. The overall findings, however, did not change significantly when looking at the online questionnaire and the interview results separately. Moreover, the responses show no significant findings related to the respondent's gender, mother's place of birth, or income, across the three domains of surveillance. There is, however, significant variations in how respondents perceived surveillance depending on their age, educational background, and labour market affiliation.

Overall, the survey shows that Danes' attitudes towards surveillance differs greatly depending on which of the three types of surveillance is involved. In general, there is great support for CCTV surveillance (83% were positive) and limited support for surveillance of e-mails and other information exchanged on the Internet (just 23% were positive) as well as for information gathered without people's knowledge (25% were positive). In relation to the third type of surveillance – "should the state have the right to gather information about everyone living in Denmark, without their knowledge" – it is important to note that the question is formulated in a rather broad manner. Compared with the first two questions, it is less clear what information gathering without people knowing entails. Is it, for example, collection of data from public registers to prevent fraud; targeted surveillance to investigate crime; or collection of information to improve public services? Respondents may thus think about different types of information and situations, whereas the first two questions are more precise. Despite these shortcomings in terms of question formulations, the survey results still indicate substantial differences in attitudes towards CCTV surveillance and the other types of surveillance, as we see below.

For CCTV surveillance and surveillance of e-mails and other information exchanged on the Internet, it is the younger population and the well-educated who are most critical of the surveillance. The oldest group (70+) is the age group where the largest proportion are positive towards CCTV surveillance. For information gathering without people's knowledge, the two oldest age groups (60–69 and 70+) are the most critical. At the same time, a bias in relation to gender can be observed in relation to this category of surveillance. On average, women are more critical than men when it comes to information gathering without people's knowledge. For all three types of surveillance, there are clear right- and left-wing tendencies, where supporters of left-wing parties are generally more critical of surveillance, except those that identify with the Social Democrats [Socialdemokratiet]. Respondents who identify with the Danish People's Party [Dansk Folkeparti], The New Right [Nye Borgerlige], Conservatives [Det Konservative Folkeparti], Liberals [Venstre], and the Liberal Alliance are the most positive towards surveillance, whereas those that identify with the Unity List [Enhedslisten] and the Alternative [Alternativet] are the most critical. The more positive attitudes towards surveillance from supporters of the Social Democrats is not surprising, as the party has marked themselves as proponents of surveillance, especially in relation to crime prevention, public order, and control of social benefits.

For all three types of surveillance, there is a correlation between attitudes towards prevention of terrorism, towards other nationalities, and towards surveillance, where those who place a high value on terrorism prevention and those who feel less trustful towards people of other nationalities are more positive towards surveillance. There is also a clear connection between institutional trust in the police and the government and the attitude towards surveillance, in the sense that people with a high degree of trust in the police and the government are more positive towards granting the state the right to surveillance of the population, across the three surveillance domains. As the survey reveals significant differences in the ways Danes assess the three types of surveillance, I now take a closer look at some of the factors that may explain these differences in attitude.

Survey results

The three surveillance domains (CCTV, e-mail and other information exchanged on the Internet, and general information gathering without people's knowledge) differ in terms of their regulation, types of exposure (Ball, 2009), character of the surveillance measure (Marx, 2006), and the privacy expectations associated with each context (Nissenbaum, 2010). In the following review, I analyse the results of the Danish Values Survey drawing on these analytical notions.

The first type, CCTV surveillance in public spaces, is regulated by the Danish act on TV-surveillance (Retsinformation, 2007). The law permits private companies and public authorities to monitor workplaces or places and premises where there is general access, such as shopping malls, schools, and hospitals; however, there is a general duty to provide information when setting up cameras in public spaces. Also, as a general rule, data must be deleted no later than 30 days after recording. As with many Europeans, Danes have become accustomed to CCTV surveillance over the years, and previous surveys have indicated a relatively high level of acceptance towards this type of surveillance among the population (Larsen, 2015). CCTV systems have been widely used by private companies to protect private property against intrusions and vandalism and by law enforcement agencies to help detect, prevent, and investigate crime and public disorder (Rajpoot & Jensen, 2015). Currently, the type of CCTV systems used in Denmark are simple recording systems that rely on monitoring by human observers. Although this may change in a future scenario with, for example, facial recognition, the amount of data captured is currently limited to CCTV footage and the retention period limited. Moreover, as a surveillance measure (Marx, 2006), CCTV systems are not bodily invasive, but rather record activities from a distance. As such, CCTV represents a more limited data processing, compared to the other two types of surveillance, and thus represents less exposure for the individual. In terms of purpose, the use of CCTV systems in public spaces is often presented as having legitimate societal goals, such as preventing crime and enhancing public security. Finally, even though few would maintain that we have no expectation of privacy when moving around in public spaces, people's expectation towards privacy is likely to be lower in public spaces, compared to the private realm (Goold, 2002). The positive attitude towards CCTV surveillance compared with the other two types of surveillance may thus be explained by the history of CCTV use (it has existed in society for a long time), its relatively limited means of data collection and exposure, a widely accepted purpose (to protect against vandalism and public disorder), and the lower expectation of privacy in public spaces.

Turning to the second type of state surveillance – that of e-mail and other information exchanged on the Internet – this is regulated by the Code of Civil Procedure (Retsinformation, 2021b) as well as the order on data retention (Retsinformation, 2021a). The data retention rules were adopted as part of Denmark's anti-terror legislation after 11 September 2001 and require telecommunications and Internet service providers to retain information about their users' communications via telephone and Internet for one year, in the interest of aiding subsequent investigations. The rules are currently under review after the Court of Justice of the European Union in 2014 found the corresponding EU-Data Retention Directive in violation of Europeans' right to privacy and ruled it invalid (EUR-Lex, 2014). The revised rules, however, maintain general data retention due to an estimation of the current security threat in Denmark. The Code of Civil Procedure gives the police access to monitor the content of citizens' communication (e.g., telephone calls, e-mails, Internet activity) in the cases of a concrete suspicion and based on a court order.

Surveillance of e-mail and other information exchanged on the Internet can be used to create a detailed profile of the individual, since it provides the state with the possibility of combining data points from a range of different sources, including social media data. As the context is everyday life, this type of surveillance may expose and combine details from a person's private world and may thus represent a more intensive level of exposure compared to CCTV surveillance. In terms of Nissenbaum's (2010) notion of contextual integrity, a person's e-mail and other information shared on the Internet may crosscut several public and private contexts. For example, e-mail communication may raise privacy expectations similar to postal mail, while other information exchanged on the Internet may compare to a range of different activities, such as searching for information in a library, walking the streets and looking at specific shops, or participating in a political meeting. The activities vary in sensitivity, and people may therefore have different privacy expectations associated with this type of surveillance; however, in general, this category represents a relatively broad scope of data collection. In terms of purpose, e-mail and other information exchanged on the Internet (connected with data retention) is often associated with legitimate societal goals, such as anti-terror measures or criminal investigation.

With the surveillance of e-mails and other information exchanged on the Internet, the state moves closer to the private sphere, and thus the encroachment on privacy can be perceived as more invasive than a CCTV camera in the public space, which may explain Danes' more critical attitude towards this type of surveillance. A general monitoring of Danes' e-mails and other information exchanged on the Internet can be used to draw a granular and detailed profile of the individual, including the social network, and is therefore likely to be experienced as more intrusive than a CCTV system that is limited to a specific physical location. Whereas there has been public debate about CCTV surveillance over the past 30–40 years, the surveillance of e-mails and Internet communication is a more recent topic of public debate. For CCTV surveillance, as well as surveillance of e-mails and other information exchanged on the Internet, it is the younger population and those with higher educations who are most critical of surveillance. This may be due to young people being less oriented towards public security and crime prevention, or, for example, placing a higher value on personal freedom than the other groups. The trend may also indicate that these groups that have grown up with communication technology and the use of the Internet generally have a more critical attitude towards state surveillance.

Regarding the third type of surveillance, information gathering without people's knowledge, the state has the authority to collect a wide range of information about people living in Denmark. In general, the Data Protection Act (Retsinformation, 2018) sets the limitations and conditions for when and how personal data can be collected. Public authorities have many opportunities to collect personal data, for example, as part of the exercise of authority. As a rule, the individual concerned should be informed about the data collection, but there are exceptions, for example, if the person is already familiar with fact that the data is being collected or if it is in relation to a police investigation.

In a society such as Denmark, in which citizens are registered from birth to death, general information gathering without people's knowledge would provide state authorities access to massive amounts of data about the individual, on everything from family relationships, health history, employment data, social benefits, and so forth. Moreover, since the information gathering would take place without the consent of the individual, the surveillance measure would be covert for those concerned. Also, it might be difficult to establish or envision a legitimate purpose for such broad and unlimited access to personal data for state authorities. The third category may thus provide individuals with extensive exposure, since they would be open to classification and scrutiny from several public registers, without their knowledge. Moreover, in line with surveillance of e-mail and Internet communication, this type of information gathering would include several sensitive contexts (family, health, work, school, social services), and might therefore be associated with high privacy expectations.

These factors may explain the rather critical attitude towards providing the state with general access to gather information without people's knowledge. Information gathering in a digital welfare state such as Denmark is potentially very intrusive and to a lesser extent associated with the purpose of public security and preventing or resolving crime, compared to CCTV or e-mail and Internet surveillance. The fact that the oldest age groups (60–69 and 70+) are the most critical towards information gathering without people's knowledge may be because this type of surveillance is associated with public security and crime prevention to a lesser degree. It may also indicate that the older groups have a stronger expectation of privacy when it comes to the state intervening without a clearly stated purpose in relation to their personal data.

The right- and left-wing tendencies that emerged for all three types of surveillance follow the political parties' general positions in the debate on surveillance, where right-wing parties are generally more positive towards surveillance and left-wing parties are more critical (except for the Social Democrats). Unlike the other parties on the left, the Social Democrats have positioned themselves as positive towards surveillance, for example, by promoting more extensive use of CCTV systems in public spaces and advocating for data retention in the fight against crime and in relation to stronger control of social benefits.

The clear connection between the attitudes towards surveillance and towards terrorism and people with other nationalities observed in the study may relate to the close interlinkage between the fight against terrorism and surveillance measures that has unfolded since 11 September 2001. For example, the surveillance of e-mails and Internet communication was originally introduced as a measure to fight terrorists, as part of Denmark's first counter-terrorism package. As such, fear of terrorism and a general feeling of unease towards "foreigners" may prompt a more positive attitude towards surveillance.

Likewise, the clear connection between a high level of trust in the police and the government and a positive attitude towards CCTV surveillance and surveillance of e-mails and Internet communication could be explained by the fact that, for many, surveillance is associated with law enforcement and the fight against crime; hence, people with great confidence in the government and the police are more positive towards granting the state this opportunity for surveillance.

Conclusion

The Danish Values Survey shows, as this chapter has illustrated, that Danes' attitudes towards surveillance varies largely depending on the type of surveillance. A large majority of Danes are in favour of CCTV surveillance, which in the public debate is often legitimised with public safety and security, while the more intrusive forms – monitoring of e-mails and other information exchanged on the Internet, as well as information gathering without people's knowledge – only have the support of about one in four Danes. Thus, there is a predominantly critical attitude towards these more invasive types of surveillance, which stands in sharp contrast to the broad support of CCTV surveillance in public spaces. Despite the Danes being relatively trustful towards the state and its institutions, the majority of people are not willing to allow state surveillance in relation to their communications, nor with respect to general information.

Even when considering the differences in age and educational background, the study shows widely agreed upon boundaries and limits vis-à-vis state surveillance in these two domains. As illustrated by the analyses, the three types of surveillance differ in terms of their regulation, the type and amount of data collected, the potential exposure that the measure may lead to, and in relation to the privacy expectations evoked, with CCTV surveillance (in its current form) being by far the least invasive measure. Three out of four Danes oppose state surveillance of their e-mails, Internet exchanges, and general information, which may reveal a detailed account of the individual and thus involve a high degree of exposure. Moreover, these types of surveillance affect the individual's private sphere and, therefore, higher privacy expectations are attached. In contrast, four out of five Danes support CCTV surveillance in public spaces, which encompasses a more limited degree of exposure and is situated in a context with lower privacy expectations. In other words, the Danes' support of, or opposition towards, surveillance largely depends on the context and characteristics of the surveillance at stake.

References

Agre, P. (1994). Surveillance and capture: Two models of privacy. *The Information Society*, *10*(2), 101–127, https://doi.org/10.1080/01972243.1994.9960162

Alston, P. (2019, October 11). *A/74/493: Digital welfare states and human rights – Report of the special rapporteur on extreme poverty and human rights*. United Nations, Human Rights Council. https://www.ohchr.org/en/documents/thematic-reports/a74493-digital-welfare-states-and-human-rights-report-special-rapporteur

Ball, K. (2009). Exposure. *Information, Communication & Society*, *12*(5), 639–657. https://doi.org/10.1080/13691180802270386

Beniger, J. R. (1986). *The control revolution: Technological and economic origins of the information society*. Harvard University Press.

Bigo, D., Isin, E., & Ruppert, E. (2019). Data politics. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 1–18). Routledge. https://doi.org/10.4324/9781315167305

Bogard, W. (2006). Welcome to the society of control. In K. D. Hagerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 55–78). University of Toronto Press.

Buhl, M. (2022). *Reaching out for the hard to reach – investigating digital exclusion of adult citizens in the Nordic countries*, 1033–1034 [Abstract from Nordic Educational Research Association 2022, Reykjavik, Iceland].

Cohen, J. E. (2013, May 20). What privacy is for. *Harvard Law Review*, *126*. https://harvardlawreview.org/2013/05/what-privacy-is-for/

Council of Europe. (1950). *European convention on human rights*. Directorate of Information. Strasbourg. https://www.echr.coe.int/documents/convention_eng.pdf

Eubanks, V. (2018). *Automating inequality – How high-tech tools profile, police and punish the poo*r. St. Martin's Press.

EUR-Lex. (2014, April 8). Judgement of the court (grand chamber). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

European Commission. (n.d.). *Shaping Europe's digital future: Denmark in the Digital Economy and Society Index*. https://ec.europa.eu/ digital-single-market/en/scoreboard/denmark

European Court of Human Rights. (2021). *Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence.* https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

Frederiksen, M. (2019a). Polarisering af danskernes tillid til hinanden [The polarising of Danes´ trust towards one another]. In M. Frederiksen (Ed.), *Usikker modernitet: Danskernes værdier fra 1981 til 2017* [*Uncertain Modernity: The Danes´ Values from 1981 to 2017*] (pp. 415–452). Hans Reitzels Forlag.

Frederiksen, M. (Ed.). (2019b). *Usikker modernitet: Danskernes værdier fra 1981 til 2017* [*Uncertain Modernity: The Danes´ Values from 1981 to 2017*]. Hans Reitzels Forlag.

Gilliom, J. (2006). Struggling with surveillance: Resistance, consciousness, and identity. In K. D. Hagerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 111–140). University of Toronto Press.

Goold, B. J. (2002). Privacy rights and public spaces: CCTV and the problem of the "unobservable observer", *Criminal Justice Ethics*, *21*(1), 21–27. https://doi.org/10.1080/0731129X.2002.9992113

Haggerty, K. D., & Ericson, R. V. (2006). The new politics of surveillance and visibility. In K. D. Haggerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 5–25). University of Toronto Press.

Harcourt, B. E. (2017). *Exposed: Desire and disobedience in the digital age*. Harvard University Press.

Hoboken, J. (2019). The privacy disconnect. In R. F. Jørgensen (Ed.), *Human rights in the age of platforms* (pp. 255–284). MIT Press.

Hækkerup, N. (2022, December 12). *Logning er en nøgle til at opklare forbrydelser – ikke masseovervågning* [*Data retention is a key to investigate crime – not mass surveillance*]. https://jyllands-posten.dk/debat/breve/ECE13617535/logning-er-en-noegle-til-at-opklare-forbrydelser-ikke-masseovervaagning/

Jørgensen, R. F. (2019). Danskernes syn på overvågning [How Danes feel about surveillance]. In M. Frederiksen (Ed.), *Usikker modernitet: Danskernes værdier fra 1981 til 2017* [*Uncertain modernity: The Danes' values from 1981 to 2017*] (pp. 143–180). Hans Reitzels Forlag.

Jørgensen, R. F. (2021). Rights and power in the digital welfare state: The case of Denmark. *Information, Communication and Society*. https://doi.org/10.1080/1369118X.2021.1934069

Kaun, A., & Dencik, L. (2020). Datafication and the welfare state: An introduction. *Global Perspectives*, *1*(1), 12912. https://doi.org/10.1525/gp.2020.12912

Koops, B-J., Newell, B. C., Timan, T., Škorvánek I., Chokrevski, T., & Galič, M. (2017). A typology of privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–575.

Larsen, J. R. (2015, February 18). Måling: Hver anden dansker vil have mere overvågning efter terror [Survey: Every second Dane wants more surveillance after terror]. *TV2 nyheder*. https://nyheder.tv2.dk/2015-02-18-maaling-hver-anden-dansker-vil-have-mere-overvaagning-efter-terror

Lauritsen, P. (2021). *Hvordan får vi et bedre overvågningssamfund?* [*How do we get a better surveillance society*]. Informations Forlag.

Lyon, D. (2003). *Surveillance after September 11*. Polity.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.

Marklund, A. (2020). *Overvågningens historie – Fra sorte kabinetter til digital masseovervågning* [*The history of surveillance – from black cabinets to digital mass surveillance*]. Gads Forlag.

Marx, G. T. (2006). Varieties of personal information as influences on attitudes toward surveillance. In D. Haggerty, & R. V. Ericson (Eds.), *The new politics of surveillance and visibility* (pp. 79–110). University of Toronto Press.

Nissenbaum, H. F. (2010). *Privacy in context – technology, policy, and the integrity of social life*. Stanford Law Books.

EU Parliament. (2000). Charter of fundamental rights of the European Union. *Official Journal of the European Communities*. https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Rajpoot, Q. M., & Jensen, C. D. (2015). Video surveillance: Privacy issues and legal compliance. In V. Kumar, & J. Svensson (Eds.), *Promoting social change and democracy through information technology* (pp. 69–92). IGI global.

Retsinformation. (2007, October 11). TV-overvågningsloven (LBK nr 1190 af 11/10/2007) [TV-surveillance act (Act nr. 1190 of 11/10/2007)]. https://www.retsinformation.dk/eli/lta/2007/1190

Retsinformation. (2018, May 23). Databeskyttelsesloven (LOV nr 502 af 23/05/2018) [Data protection act (Act no. 502 of 23/05/2018)]. https://www.retsinformation.dk/eli/lta/2018/502

Retsinformation. (2021a, March 29). Bekendtgørelse om opbevaring af registrerings- og opbevaringspligtige oplysninger (BEK nr 379 af 29/03/2021) [Order on the storage of information subject to registration and storage (Act no. 379 of 29/03/2021)]. https://www.retsinformation.dk/eli/lta/2022/379

Retsinformation. (2021b, September 15). Retsplejeloven (LBK nr 1835 af 15/09/2021) [Code of civil procedure (Act no. 1835 of 15/09/2021)]. https://www.retsinformation.dk/eli/lta/2021/1835

Schou, J., & Hjelholt, M. (2019). Digitalizing the welfare state: Citizenship discourses in Danish digitalization strategies from 2002 to 2015. *Critical Policy Studies*, *13*(1), 3–22. https://doi.org/10.1080/19460171.2017.1333441

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Statistics Denmark. (2019). *It-anvendelse i befolkningen 2019* [*Analysis of IT-usage among the population 2019*]. Statistics Denmark.

Vanberg, A. D. (2021). Informational privacy post GDPR – end of the road or the start of a long journey? *The International Journal of Human Rights*, *25*(1), 52–78. https://doi.org/10.1080/13642987.2020.1789109

Wood, D. M., & Webster, C. W. R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, *5*(2), 259–273. **https://doi.org/**10.30950/jcer.v5i2.159

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.

Endnotes

[1] The examination of survey data is based on Jørgensen (2019).

[2] See, for example, this intervention by the former Minister of Justice, Nick Hækkerup, in the public debate on data retention as "mass surveillance" from January 2022 (Hækkerup, 2022).

[3] By "digital welfare state", I refer to a state in which public authorities deploy technologies to perform a broad range of public services, such as social protection and assistance systems, public education, and healthcare, as described, for example, by Alston (2019).

[4] The Digital Economy and Society Index (DESI) ranks Denmark as the highest performing country in Europe. The EU digital scoreboard presents Denmark as a world leader in digital progress (see European Commission, n.d.).

[5] For an elaboration of the survey method and statistical validity, see Jørgensen (2019), especially the Appendix.

CHAPTER 6

Accepting or rejecting online surveillance

The case of Swedish students

LARS SAMUELSSON

DEPARTMENT OF HISTORICAL, PHILOSOPHICAL AND RELIGIOUS STUDIES, UMEÅ UNIVERSITY, SWEDEN

ABSTRACT

This chapter is based on the results of a questionnaire that was distributed to students at Umeå University, Sweden, and investigates their propensity to accept online surveillance in relation to three conditions that could increase their acceptance of it: 1) that it results in personal benefits; 2) that they have consented to it; and 3) that society can benefit from it. To categorise the respondents' positions, I use a conceptual apparatus from moral philosophy, namely, the distinction between deontological and consequentialist ethical views. The study reveals two clear tendencies among the respondents: The most considerable difference among them is a difference in their general attitudes to being surveilled online rather than a difference in ethical thinking of a kind that can be framed in terms of deontology and consequentialism; the personal benefits that can result from allowing online surveillance do not generally have any significant impact on their acceptance of it.

KEYWORDS: online surveillance, ethics of surveillance, personal data, societal benefits, consent

Samuelsson, L. (2023). Accepting or rejecting online surveillance: The case of Swedish students. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 125–144). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-6

Introduction

This chapter concerns people's acceptance of online surveillance – here equated with the storing, using, and sharing of personal data that is gathered online, where any kind of information about a person counts as personal data (compare with Fuchs, 2017; Leckner, 2018; Lyon, 2014). Many studies have shown that people care about their privacy and dislike being surveilled.[1] Yet, there may be circumstances that would increase their acceptance of online surveillance. Providers of commercial online services, such as social media platforms and smartphone apps, may hope that people's acceptance of being surveilled increases if they have consented to their data being stored and shared – typically by ticking a box to accept the provider's terms of agreement. They may also hope that people judge the benefits of using their services to outweigh any inconveniences of being surveilled and thus find the surveillance associated with using the services acceptable. Governmental organisations who collect data about people for health or security purposes, for instance, may hope that people's acceptance of being surveilled increases if surveillance leads to societal benefits.

The study on which this chapter builds was motivated by the question of how different considerations may increase people's acceptance of online surveillance. I have chosen to use three broad categories for classifying such considerations: self-interested, consequentialist, and deontological considerations. The latter two categories are borrowed from moral philosophy. According to consequentialist ethical theories, moral justification is a matter of reaching good outcomes (e.g., societal benefits). Deontological theories, on the other hand, typically stress the importance of respecting persons, which requires not enforcing something – like surveillance – on them without their authentic, genuine, and informed consent.

The use of this categorisation is motivated by how debates about the justification of surveillance tend to unfold. As noted above, personal benefits on the part of the surveilled person may be thought to increase their acceptance of being surveilled (self-interested considerations). It is a common assumption that human beings are largely driven by self-interest.[2] Perhaps, then, people's propensities to accept online surveillance are also largely explained by what they believe they can gain from allowing it. However, in addition, discussions about the justification of surveillance typically centre around two main *ethical* perspectives (see Macnish, 2022). The first stresses the potential positive outcomes of surveillance: If the consequences of surveillance – usually in terms of societal benefits – are good enough, this may render it acceptable (consequentialist considerations). The second perspective stresses respect for persons, often framed in terms of respect for their privacy: Surveillance is deemed acceptable to the extent that it respects the persons who are being surveilled – which is generally taken to require that they have authentically, genuinely, and informedly consented to it (deontological considerations). The three categories used in this chapter thus capture the main considerations typically referred to in discussions about the justification of online surveillance.

The purpose of the study was to look for patterns in people's views on the acceptability of online surveillance. To what extent do certain considerations increase their acceptance of being surveilled? Can we find a clear division of groups of people that display different kinds of ethical thinking, and thus regard different considerations as important for their acceptance of online surveillance? Or is it common that people assign roughly the same importance to different considerations? And so on. In order to begin to approach these (and other) questions, a questionnaire was distributed to students at Umeå University, Sweden, with questions about online behaviour, privacy, perceived threats, and views on online surveillance. 956 students answered the survey over a period of six months, between November 2019 and May 2020.

My specific aim with this chapter is to contribute to the understanding of what young people in Sweden think about the acceptability of online surveillance in relation to the three considerations identified above. These considerations were represented by the following three conditions, each of which could then be plausibly thought to increase the respondents' acceptance of online surveillance: 1) that it results in personal benefits; 2) that they have consented to it; and 3) that society can benefit from it. While there are many studies – in Sweden and elsewhere – of people's online behaviour, and of their views, attitudes, and motivations concerning privacy and being surveilled (see endnote 1), the same attention has not been paid to people's propensity to regard online surveillance as acceptable under various considerations. Yet, an increased understanding of this can provide important insights for decision- and policy-makers – as well as for people constructing and developing various online services (such as social media services, smartphone apps, online shopping services, communication services, etc.) – about what is important to people when it comes to their acceptance of having their personal information stored and shared.

The disposition of the chapter is as follows: In the next section, I detail the theoretical points of departure for the study, including the categories of deontological and consequentialist considerations. I then go on to explain the research procedure and method used, before first presenting and then discussing the relevant survey results.

Theoretical points of departure

The ongoing digital transformation of society has resulted in what David Lyon (2018: 30) refers to as a "culture of surveillance": "the everyday webs of social relations, including shared assumptions and behaviours, existing among all actors and agencies associated with surveillance". In contrast to traditional top-down surveillance, where a state or other entity with authority constitutes the surveilling agent – Bentham's (1995) Panopticon providing a powerful illustration – surveillance is nowadays to a large extent a more horizontal, sometimes even reciprocal, affair, where many citizens possess the means to surveil each other. In addition, large companies and various organisations have much to gain from collecting information about people, for instance, to use consumer and social media data for marketing purposes (Ball, 2017; Colaresi, 2020; Zuboff, 2019). This situation has been referred to in terms such as new surveillance (Marx, 1998), soft surveillance (Marx, 2005), surveillance capitalism (Zuboff, 2019), and surveillance culture (Lyon, 2014, 2017) – a common denominator being the perception that such surveillance is something that we live in, that surrounds us, and that we need to relate to in one way or another. This comparatively new situation highlights the ethical issue of under what conditions or circumstances surveillance may be deemed acceptable.

Typically, when the justification of surveillance is discussed, two main perspectives are contrasted: voluntariness to be surveilled, or to have one's privacy infringed upon (i.e., to have one's information stored and shared), versus the expected societal benefits of surveillance (see Macnish, 2022). These two perspectives map onto the two main types of moral theory in moral philosophy (here understood as theories about what makes actions right or wrong): deontological theories and consequentialist theories.[3]

Although the group of deontological theories is diverse, and often characterised negatively (more or less as non-consequentialism) it is characteristic of such theories that they in one way or another stress the importance of respect for persons (see Alexander & Moore, 2021; see also Rentmeester, Chapter 9). Such respect is normally taken to require that people are not treated in ways to which they have not given their authentic, genuine, and informed consent (at least unless these ways of treating them are completely unproblematic from a moral point of view). If a person has not consented to personal information being stored and shared, then – other things being equal – storing and sharing the information is generally considered a morally objectionable privacy infringement (e.g., DeCew, 2018). However, if a person authentically, genuinely, and informedly consents to their privacy being infringed upon, a deontologist would typically regard such a privacy infringement as justified. In such a case, the requirement of voluntariness has been met; the person has given their permission to being treated in a way that would have otherwise been disrespectful (see also Miller & Wertheimer, 2010; Müller & Schaber, 2018).

According to a consequentialist theory, on the other hand, the only thing that matters to whether an action is right or wrong is the outcome of that action and how the (expected) value of that outcome compares to the (expected) values of the outcomes of alternative (possible) actions (e.g., Sinnott-Armstrong, 2021).[4] Whether an instance of surveillance is justified is then largely a question of whether it is beneficial to society (assuming that it is also beneficial to the people constituting the society).

This picture is simplified in several ways. As already noted, there are many kinds of deontological theory, and a deontologist can believe that some kinds of actions are exempt from the transformational power of voluntariness (i.e., that there are certain kinds of actions that are not justified, even if they have been authentically, genuinely, and informedly consented to). One may think that surveillance, or privacy infringements, belong to this group of actions. There may also be deontological considerations relevant to the acceptability of online surveillance other than those relating to voluntariness, and deontologists may in various ways assign some importance to consequences (for further complications in the ethics of surveillance, see Macnish, 2018). Moreover, there are pluralist ethical theories involving both deontological and consequentialist elements. However, none of these complications are important in relation to the purpose for which I invoke the categories of deontological and consequentialist ethical thinking. Most people display both kinds of thinking, and my purpose is to reveal patterns in people's propensities to accept online surveillance: Can we, for instance, distinguish different groups where different modes of ethical thinking dominate?

Method and research procedure

As mentioned in the introduction, this study is based on a survey of students (either present or very recently so) at Umeå University, Sweden. The survey had the form of an online questionnaire, which was distributed to several large present and recent student groups on their online learning platforms. Between November 2019 and May 2020, 956 students answered the questionnaire, which contained questions about online behaviour, privacy, perceived threats, and attitudes to online surveillance. The sample comprised campus-based students as well as online students from a variety of subjects and study programmes, such as teacher education, philosophy, informatics, and engineering.

The survey tool used was Websurvey by Textalk, provided by Umeå University (to ensure secure storing in line with the GDPR regulations). The students were invited to participate anonymously and voluntarily, and they were not offered any rewards for participating. This research procedure generated a high number of responses, but at the cost of a low (and unknown) response rate (since we do not know how many students our invitation reached).[5]

For the survey questions about attitudes, behaviours, beliefs, views, or opinions, we used an 11-point scale (ranging from 0 to 10), on which the respondents marked the alternative which they thought best represented themselves on the issue in question (with 0 representing the lowest possible value and 10 the highest). The main reason for using this scale was to be able to compare our results with other similar studies using the same scale (see Svenonius & Björklund, 2018).

The survey was conducted within the larger research project "iAccept: Soft surveillance – between acceptance and resistance", and hence the study presented in this chapter covers only parts of the survey results (for a more comprehensive overview of the survey, see Cocq et al., 2020). When we – the research team of iAccept – designed the survey, two considerations in particular guided our selection of survey questions: We wanted to be able to compare our results with the results of other studies that we found relevant to our project (e.g., Svenonius & Björklund, 2018; Sønderskov & Dinesen, 2016), and we wanted to complement earlier studies with questions that had not been as thoroughly investigated. In particular, we formulated questions about the respondents' acceptance of online surveillance, intended to capture the three considerations outlined above: self-interested, deontological, and consequentialist. The following question was posed in the questionnaire:

> To what extent would the following conditions increase your acceptance of your personal data being stored and shared when you are online? [where 0 represents "not at all" and 10 represents "to 100%"].

The conditions we asked the respondents to take a stand on were the following:

> Condition 1: "That it is a precondition for others to develop and give you access to desirable services" (a self-interested consideration).
>
> Condition 2: "That you receive personal, customised offers and search results (based on your previous online activities)" (a self-interested consideration).
>
> Condition 3: "That it facilitates some of your online activities (access to various services, online shopping, etc.)" (a self-interested consideration).
>
> Condition 4: "That you are able to consent to your data being stored and shared when you choose to use a certain service" (a deontological consideration).
>
> Condition 5. "That society can benefit from the data about you that is being stored (e.g., to combat criminality/terrorism or achieve health benefits)" (a consequentialist consideration).

Due to the variety of possible self-interested considerations in this area, we chose to divide them into three different conditions to minimise the risk of missing some consideration deemed important by people. Of course, we could have made even more fine-grained distinctions with respect to all three kinds of considerations, but we wanted to avoid a more cumbersome questionnaire, and we judged these formulations to capture the three intended categories well enough.

In order to expose potential patterns in the respondents' propensities to accept online surveillance and reveal possible correlations – or lack thereof – between different motivations for accepting online surveillance, I filtered the consent responses with the societal benefits responses, and vice versa, to see how the respondents' acceptance propensity under the consent condition (Condition 4) co-varied with their acceptance propensity under the societal benefits condition (Condition 5). This filtering of survey results provides an important basis for the coming discussion.

It is important to emphasise that our purpose with the survey was not to draw conclusions about the proportion of Swedish students in general holding certain views, but to track *patterns* among the respondents – in particular, to reveal striking correlations between an individual's answers to different questions – as a way of beginning to approach the issue of how young Swedes think about questions relating to online surveillance. Thus, my goal in this chapter is not to provide a regular statistical analysis of the results, and they have not been treated according to strict statistical methods. The procedure we used for distributing the questionnaire does not allow for that, and we do not find such a treatment of the results relevant to the limited purpose of looking at the particular group that answered the survey – with a focus on correlations between answers. The results are used to provide a point of departure for the coming discussion.

Although the respondents in this study constitute a limited sample – all of them being students at one university in one country – we took them to represent an interesting part of the population to look at: mostly young, relatively well-informed (regarding computers, the Internet, online services, etc.) citizens, who, arguably, are also an important target group for many prominent online services (like social networks and shopping services). The background of the respondents allows us to assume that they are generally comparatively experienced users of computers, other digital devices, and online services. In this respect, Swedes in general stand out from an international perspective, displaying a very high usage of both the Internet and social media (DataReportal, 2020). Compared with most people in the world (and probably in Sweden as well), we believe our respondents can be expected to have a good understanding of the kind of online surveillance we asked them about.

Survey results

Before addressing the results that are at the focus of this study, let me first briefly reveal some background survey data that may facilitate the assessment of the main results.

Background data

The declared gender distribution of our respondents is 60 per cent women and 39 per cent men (1% identified as neither), although it differs somewhat across different courses and programmes. 57 per cent of the respondents were current students while 36 per cent were working. 60 per cent were 20–29 years old, 31 per cent were 30–49, 7 per cent were over 50, and 2 per cent were under 20.

The respondents generally reported a high degree of social media usage. 79 per cent claimed to use Facebook at least a few times a week (58% daily), and 85 per cent claimed to use Messenger at least a few times a week (62% daily). Online privacy was considered important to most of the respondents. In response to the claim "It is important for me that what I do online is private/anonymous", 79 per cent marked one of the alternatives 5 to 10 on the 11-point scale described above. At the same time, the survey results reveal that the respondents generally did not do much to hide their data: Only 23 per cent stated that they sometimes use a VPN (virtual private network) service; 10 per cent that they sometimes use web browsers that do not store search results; and 37 per cent that they sometimes cover their computer's camera. 45 per cent of the respondents reported that they sometimes apply private mode in their web browser; however, that measure only conceals data locally on the computer.

To summarise, the group of respondents generally consists of young, experienced social media users who regard their privacy as important, but who do not do very much to protect it when they are online.

Acceptance of online surveillance

Let us now turn to the results focusing on the acceptance of online surveillance. Table 6.1 shows the unfiltered results for the conditions that we asked about. The first Conditions 1–3 target self-interest and concern potential personal benefits of online surveillance (and will be referred to as "the personal benefits conditions"), Condition 4 concerns consent (and will be referred to as "the consent condition"), and Condition 5 concerns societal benefits (and will be referred to as "the societal benefits condition").

Table 6.1 Acceptance increase of personal data being stored and shared (per cent)

Condition	Modest increase (0–3)	Medium increase (4–6)	Strong increase (7–10)	No opinion	No answer
1. That it is a precondition for others to develop and give you access to desirable services.	43	32	15	10	0
2. That you receive personal, customised offers and search results (based on your previous online activities).	62	24	9	4	0
3. That it facilitates some of your online activities (access to various services, online shopping, etc.).	42	32	21	5	0
4. That you are able to consent to your data being stored and shared when you use a certain service.	28	25	43	4	0
5. That society can benefit from the data about you that is being stored (e.g., to combat criminality/terrorism or achieve health benefits).	20	32	43	6	1

Comments: The question was posed "To what extent would the following conditions increase your acceptance of your personal data being stored and shared when you are online? [where 0 represents "not at all" and 10 represents "to 100%"]". For each condition, the table shows the percentage (rounded to the closest integer) of respondents who marked the respective response alternatives (here merged into "modest increase", "medium increase" and "strong increase") or who reported having no opinion or chose not to respond.

Table 6.1 reveals that the consent condition and the societal benefits condition stand out in the sense that they generally make a larger difference with respect to the respondents' acceptance propensity of online surveillance than the three conditions that concern personal benefits. Looking at "the strong increase interval", we find 15 per cent of the respondents within this interval for Condition 1; 9 per cent for Condition 2; and 21 per cent for Condition 3. The number is considerably higher for the consent condition and the societal benefits condition, namely 43 per cent for both. A corresponding pattern emerges on the other side of the scale. If we look at "the modest increase interval", we find for the personal benefits conditions 43 per cent of the respondents within this interval for Condition 1; 62 per cent for Condition 2; and 42 per cent for Condition 3. For the consent condition, the number is 28 per cent, and for the societal benefits condition, it is 20 per cent – both numbers considerably lower than those we see for the three personal benefits conditions.

Correlations between consent responses and societal benefits responses

In order to reveal potential patterns in the respondents' acceptance increase with regard to the consent condition and the societal benefits condition, I filtered the consent responses with the societal benefits responses, and vice versa. This makes it possible to reveal correlations between responses. We get to see how respondents within the different intervals for one of these conditions responded with respect to the other. Again, I use the three intervals referred to as "the modest increase interval" (0–3), "the medium increase interval" (4–6), and "the strong increase interval" (7–10) to present the results.

It is worth pointing out that by using these intervals, I am not comparing equal intervals. However, I do not see this as problematic in relation to the kind of correlation I want to track. The comparison is simply made on the assumptions that respondents who find a condition notably important to their acceptance of being surveilled would tick one of the alternatives 7–10, that respondents who do not find the condition in question important to a notable degree would choose an alternative in the interval 0–3, and that the alternatives 4–6 are plausibly considered middle alternatives. That the intervals are not equal does not affect these assumptions, but it is important to keep in mind that interpretations of answers to questionnaires using scales with alternatives that are merely represented with numbers always rely on such assumptions.

Tables 6.2 and 6.3 show the filtering of consent condition responses with societal benefits condition responses, and vice versa.

Table 6.2 How respondents in the respective consent intervals responded about the societal benefits condition (per cent)

Interval for the consent condition	**Interval 0–3 (modest acceptance increase) for societal benefits**	**Interval 4–6 (medium acceptance increase) for societal benefits**	**Interval 7–10 (strong acceptance increase) for societal benefits**
0–3 (modest acceptance increase) (*N* = 267)	47	27	24
4–6 (medium acceptance increase) (*N* = 238)	9	46	41
7–10 (strong acceptance increase) (*N* = 414)	9	28	58
Total (*N* = 956)	20	32	43

Comments: The table shows how the respondents in the different intervals for the consent condition responded with regard to the societal benefits condition. The numbers reveal the percentage (rounded to the closest integer) of respondents in the respective intervals for the consent condition that are found in the different intervals for the social benefits condition (e.g., the number 47 in the upper left cell reveals that 47% of the 267 respondents with modest acceptance increase regarding the consent condition show modest acceptance increase also with regard to the societal benefits condition). The last row shows how the total number of respondents were distributed over these intervals for the societal benefits condition.

Table 6.3 How respondents in the respective societal benefits intervals responded about the consent condition (per cent)

Interval for the societal benefits condition	Interval 0–3 (modest acceptance increase) for consent	Interval 4–6 (medium acceptance increase) for consent	Interval 7–10 (strong acceptance increase) for consent
0–3 (modest acceptance increase) (*N* = 187)	67	11	21
4–6 (medium acceptance increase) (*N* = 302)	24	36	38
7–10 (strong acceptance increase) (*N* = 408)	16	24	59
Total (*N* = 956)	28	25	43

Comments: The table shows how the respondents in the respective intervals for the societal benefits condition responded with regard to the consent condition. The numbers reveal the percentage (rounded to the closest integer) of respondents in the respective intervals for the societal benefits condition that are found in the different intervals for the consent condition. The last row shows how the total number of respondents were distributed over these intervals for the consent condition.

Tables 6.2 and 6.3 reveal similar patterns: Respondents with modest acceptance increase with regard to one of the conditions tend to demonstrate modest acceptance increase with regard to the other; respondents with medium acceptance increase with regard to one of the conditions tend to demonstrate medium acceptance increase with regard to the other; and respondents with strong acceptance increase with regard to one of the conditions tend to demonstrate strong acceptance increase with regard to the other. The relevant numbers are in the light grey shadowed cells. The only minor exception to this pattern is in table 6.3, where the largest proportion of the respondents in the medium acceptance increase interval for the societal benefits condition are found in the strong acceptance increase interval for the consent condition (the dark grey shadowed cell), but it is only two percentage points larger than the proportion found in the medium acceptance increase interval.

The filtering of results also reveals that of the total number of respondents (956), 240 (25%) are found in the strong acceptance increase interval for both the consent condition and the societal benefit condition, while 125 respondents (13%) are found in the modest acceptance increase interval for both conditions.

To summarise the above, a large proportion of the respondents fit the following pattern: To the extent that one of the conditions increases (or fails to increase) their acceptance of being surveilled online, the other condition does so (or not) as well.

At the same time, however, a noteworthy number of respondents demonstrate an opposite pattern: 24 per cent of the respondents in the modest acceptance increase interval for the consent condition are in the strong acceptance increase interval for the societal benefits condition (see Table 6.2); 21 per cent of the respondents in the modest acceptance increase interval for the societal benefits condition are in the strong acceptance increase interval for the consent condition (see Table 6.3); 9 per cent of the respondents in the strong acceptance increase interval for the consent condition are in the modest acceptance increase interval for the societal benefits condition (see Table 6.2); and 16 per cent of the respondents in the strong acceptance increase interval for the societal benefits condition are in the modest acceptance increase interval for the consent condition (see Table 6.3). The filtering of results reveals that of the total number of respondents (956), 65 (7%) are found in the strong acceptance increase interval for the societal benefits condition *and* the modest acceptance increase interval for the consent condition, while 39 respondents (4%) are found in the modest acceptance increase interval for the societal benefits condition *and* the strong acceptance increase interval for the consent condition.

Hence, among the respondents, there are also noteworthy, but smaller, groups of people who regard only one of the conditions as considerably important to their acceptance of online surveillance, and thus seem to display an ethical thinking with *either* a clear deontological *or* a clear consequentialist tendency (with respect to their acceptance of online surveillance).

Discussion

The survey results reveal two rather clear tendencies among the respondents: 1) the kind of personal benefits that can be gained from allowing the storing and sharing of personal information do not generally significantly increase their acceptance of being surveilled; and 2) respondents whose acceptance of online surveillance remains largely unaffected under the consent or societal benefits condition also reported that their acceptance remains largely unaffected under the other (and correspondingly for those respondents whose acceptance is instead largely affected under these conditions). Let us start by considering these two tendencies in turn.

Personal benefits

Even if one gets better, simpler, or more personalised services as a result of the storing and sharing of one's personal information, that is not generally taken to make the storing and sharing of one's personal information significantly more acceptable among our respondents (but we should bear in mind the possibility that more fine-grained descriptions of personal benefits would have yielded a somewhat different result). As the background data revealed, the respondents do indeed – to a large extent – use services that store and share their data when they are online (e.g., Facebook and Google), and the motivation for using such services is arguably for the most part precisely that one hopes to receive some kind of personal benefit. How should we understand these results?

It is quite possible that many people think that even if they get the kind of benefits they sought, and even if they voluntarily signed up for the service in question, this is still not sufficient to justify the kind of online surveillance associated with receiving these benefits. Perhaps they think it is also required that they explicitly consent to being surveilled (the deontological consideration), or that the surveillance has other positive effects (the consequentialist consideration), or perhaps they would not consider it acceptable in any circumstances. It is, after all, a common phenomenon that people take part in a practice they deem unacceptable when and because it is in their interest to do so.

It is also quite possible that many people do not believe that the amount of online surveillance performed by the provider of the service in question is really required to give them the kind of benefits they hope to receive by using the service.

Consent and societal benefits

Respondents with a strong acceptance increase regarding the consent condition also tended to show a strong acceptance increase with regard to the societal benefits condition, and vice versa. The same pattern holds for medium and modest acceptance increase as well. Hence, rather than seeing a clear pattern in differences in ethical thinking among the respondents, we see a clear pattern in differences in the general stability of their acceptance of online surveillance.

As the "Total" rows in Tables 6.2 and 6.3 show, we find the largest groups of respondents in the strong acceptance increase interval for both the consent condition and the societal benefits condition (43% in both cases). And, as we have seen, in both these groups, it is most common to belong to the other group as well (25% of the total number of respondents are found in both). Hence, for many of our respondents, whether they have consented to it and whether society can benefit from it does make a considerable difference to their acceptance of being surveilled online. These considerations can indeed increase people's acceptance of online surveillance.

As for the modest acceptance increase interval, the proportion of respondents found in this interval for the two conditions is not insignificant (28% for the consent condition and 20% for the societal benefits condition). Again, as we have seen, in both groups it is most common to belong to the other group as well (13% of the total number of respondents belong to both groups). So, we also have a fairly significant group of people whose acceptance of online surveillance is largely unaffected by either of the ethical considerations – the deontological one, focusing on consent, and the consequentialist one, focusing on societal benefits.

These results indicate that the most considerable difference among the respondents is a difference in their general attitude to being surveilled online – that is, in how worried, suspicious, or concerned they are about having their personal data stored and shared – rather than a difference in ethical outlook that can be framed in terms of deontological and consequentialist ethical thinking. Some other findings that can be gathered from our survey results may strengthen this interpretation: A filtering of the relevant results revealed that for both the consent condition and the societal benefits condition, respondents in the modest acceptance increase interval reported a significantly lower level of trust in various institutions, as well as in other people, than did respondents in the strong acceptance increase interval. This fits well with the picture that the difference between these groups is largely a matter of various degrees of suspicion and worry about surveillance. Moreover, our survey revealed that those in the modest acceptance increase interval (for both conditions) were more worried about surveillance in general than those in the strong acceptance increase interval, indicating that if you are worried about surveillance to begin with, your acceptance of online surveillance will not easily increase under the conditions we queried about. This pattern was strongest in the case of the societal benefits condition. A possible interpretation is that societal benefits of surveillance seem less pivotal if you also think that surveillance comes with significant risks or societal harms. Lastly, if we look at the medium acceptance increase interval, we see that we have quite a large group whose acceptance of online surveillance is moderately affected by both conditions (see Tables 6.2 and 6.3), indicating that they are not led by ethical thinking that targets one of these conditions in particular.

Differences in ethical thinking

As we saw in the results section (see Tables 6.2 and 6.3), a noteworthy proportion of the respondents demonstrate a different pattern. For instance, 24 per cent of the respondents in the modest acceptance increase interval for the consent condition are in the strong acceptance increase interval for the societal benefits condition, and 21 per cent of the respondents in the modest acceptance increase interval for the societal benefits condition are in the strong acceptance increase interval for the consent condition. So, here we have groups of respondents whose acceptance of online surveillance is largely affected by one of the conditions, but not by the other.

The difference between these groups could, to some extent, be explained by a difference in ethical outlook (which can be framed in terms of deontological and consequentialist ethical thinking). People whose acceptance of online surveillance largely increases under the societal benefits condition, but not under the consent condition, display a typical consequentialist outlook (which is compatible with embracing other kinds of ethical thinking as well), while people whose acceptance of online surveillance largely increases under the consent condition, but not under the societal benefits condition, display a typical deontological outlook (which is compatible with embracing other kinds of ethical thinking as well).

Some problematising remarks

I end my discussion of the results by providing some problematising remarks. First, it should be noted that we only asked about *increases* in the respondents' acceptance of online surveillance in our survey; we did not ask about their initial views. Perhaps the reason why someone would not increase their acceptance of online surveillance under the conditions we asked about is that their acceptance was already very high; however, this possibility can hardly provide a significant part of the explanation of our results. As noticed above, respondents in the modest acceptance increase interval (for both the consent condition and the societal benefits condition) were generally most worried about surveillance. Furthermore, it has been confirmed in numerous studies that people in general care about their privacy and do not want to be surveilled (see, e.g., Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017), a result that was also confirmed in our own survey through the question about attitudes towards privacy (as accounted for in the results section above).

Second, one may question the strength of the connection between the two conditions I have focused on and the two kinds of ethical thinking – deontological and consequentialist. In particular, consent may be seen as a personal, self-interested matter, rather than an ethical matter, if it is taken as implicit that you consent to something only if you have something to gain from it. However, given the clear difference in general acceptance increase that we saw between the consent condition and the three personal benefits conditions, this does not seem to be a plausible interpretation of the survey results.

It is difficult to ask directly about people's ethical thinking in a questionnaire survey – for one thing, people in general are not familiar with concepts such as consequentialism and deontology – so instead we had to approach the issue indirectly, via the questions about consent and societal benefits. A further interesting step would be to, for instance, conduct interviews with respondents to allow more nuanced reasoning about which ethical (and other) considerations are relevant to their acceptance of online surveillance, and thus increase the understanding of motives for accepting or rejecting it.

Related to the previous note (and as accounted for in the methods section), our sample was rather limited. It would of course be interesting to investigate the views of other groups of people (e.g., other age groups) and people in other countries.

Finally, we may have missed some important consideration that is relevant to people's acceptance of online surveillance (or not used fine-grained enough characterisations of personal and societal benefits). We asked about five conditions, but there may certainly be more (both ethical and personal).

Our questionnaire did have the answering-alternative “something else” in addition to the five conditions, but only 1 per cent of the respondents are found in the strong acceptance increase interval for “something else”. Of course, this does not mean that we can say that the respondents did not consider any other considerations important to their acceptance of online surveillance (as they were led by the alternatives we gave them), but at least we did not miss anything that the respondents spontaneously pointed out. In any case, it would certainly be interesting to perform a more comprehensive and fine-grained study of precisely which considerations affect people’s acceptance of online surveillance.

Conclusion

The most prominent findings of this study can be summarised as follows: The kind of personal benefits that can be gained by allowing the storing and sharing of personal information does not generally significantly increase the acceptance of online surveillance among the respondents of our questionnaire survey (at least not the benefits we asked about; see Table 6.1). While we find a larger number of respondents in the strong acceptance increase interval than in the modest acceptance increase interval with respect to both the consent condition and the societal benefits condition, there is also a significant group of people in the modest acceptance increase interval for each of these conditions. Moreover, many of them are found in the modest acceptance increase group for both conditions. Thus, given the views of our respondents, it seems that the only way for online service providers to gain *broad* acceptance of their services is to be restrictive with the storing and sharing of personal data. Many people are opposed to online surveillance, irrespective of which conditions are met.

As for those people who can be sorted into different ethical groups, different measures are required to gain their acceptance of being surveilled online: To some, it is important that they have given their consent to this surveillance; to others, it is important that it contributes to societal benefits. Among the people in the latter group, it is unlikely that social media platforms (such as Facebook and Instagram) and online communication services (such as Messenger and WhatsApp) are considered to meet this requirement. The fact that people use a certain service does not imply that they consider everything about it acceptable – or justified. They may use it for self-interested reasons but still find it (ethically) objectionable.

Acknowledgements

This chapter was written as part of the project “iAccept: Soft Surveillance – Between Acceptance and Resistance” (MAW 2016.0092), funded by the Marcus and Amalia Wallenberg Foundation. I want to thank Coppélie Cocq, Jesper Enbom, and, in particular, Stefan Gelfgren for valuable input.

References

Alexander, L., & Moore, M. (2021). Deontological ethics. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2021 ed.). https://plato.stanford.edu/archives/win2021/entries/ethics-deontological/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Ball, K. (2017). All consuming surveillance: Surveillance as marketplace icon. *Consumption Markets & Culture*, *20*(2), 95–100. https://doi.org/10.1080/10253866.2016.1163942

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/j.tele.2017.04.013

Bentham, J. (1995). *The panopticon writings*. Verso Books.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, *48*(7), 953–977. https://doi.org/10.1177/0093650218800915

Cocq, C., Gelfgren, S., Samuelsson, L. & Enbom, J. (2020). Online surveillance in a Swedish context. *Nordicom Review*, *41*(2), 179–193. https://doi.org/10.2478/nor-2020-0022

Colaresi, M. (2020). How our misunderstanding of the digital and computing revolutions puts democracy at risk (and what to do about it). *Critical Quarterly*, *62*(1), 70–80. https://doi.org/10.1111/criq.12522

DataReportal. (2020). *Digital 2020: Global digital overview/digital 2020: Sweden*. https://datareportal.com/

DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Spring 2018 ed.). https://plato.stanford.edu/archives/spr2018/entries/privacy/

Fuchs, C. (2017). *Social media: A critical introduction* (2nd ed.). Sage.

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77,* 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64,* 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Leckner, S. (2018). Sceptics and supporters of corporate use of behavioural data: Attitudes towards informational privacy and Internet surveillance in Sweden. *Northern Lights*, *16*(1), 113–132. https://doi.org/10.1386/nl.16.1.113_1

Lyon, D. (2014). The emerging surveillance culture. In A. Jansson, & M. Christensen (Eds.), *Media, surveillance and identity: Social perspectives* (pp. 71–90). Peter Lang.

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 824–842. https://ijoc.org/index.php/ijoc/article/view/5527

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity Press.

Macnish, K. (2018). *The ethics of surveillance: An introduction*. Routledge. https://doi.org/10.4324/9781315162867

Macnish, K. (2022). Surveillance ethics. In *Internet encyclopedia of philosophy*. https://iep.utm.edu/surv-eth/

Madden, M., & Rainie L. (2015). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Marx, G. T. (1998). Ethics for the new surveillance. *The Information Society*, *14*, 171–185. https://doi.org/10.1080/019722498128809

Marx, G. T. (2005). Soft surveillance: Mandatory voluntarism and the collection of personal data. *Dissent*, *52*(4), 36–43. https://doi.org/10.1353/dss.2005.0074

Miller, F. G., & Wertheimer, A. (Eds.). (2010). *The ethics of consent: Theory and practice*. Oxford University Press.

Müller, A., & Schaber, P. (Eds.). (2018). *The Routledge handbook of the ethics of consent*. Routledge. https://doi.org/10.4324/9781351028264

Sinnott-Armstrong, W. (2021). Consequentialism. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Fall 2021 ed.). https://plato.stanford.edu/archives/fall2021/entries/consequentialism/

Svenonius, O., & Björklund F. (2018). Explaining attitudes to secret surveillance in post-communist societies. *East European Politics*, *34*(2), 123–151. https://doi.org/10.1080/21599165.2018.1454314

Sønderskov, K. M., & Dinesen. P. T. (2016). Trusting the state, trusting each other? The effect of institutional trust on social trust. *Political Behavior*, *38*(1), 179–202. https://doi.org/10.1007/s11109-015-9322-8

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

Endnotes

[1] Consider, for instance, the vast literature on the so-called privacy paradox (three comprehensive critical literature reviews are Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). Illustrative overviews concerning people's online behaviours and attitudes to online surveillance can be found by Auxier and colleagues (2019), Boerman and colleagues (2021), and Madden and Rainie (2015). For studies in a Swedish context, see, for instance, Cocq and colleagues (2020) and Leckner (2018). The present study is not concerned with the different reasons people may have for disliking being surveilled, but with the question of whether there are considerations that could increase their acceptance of online surveillance.

[2] In relation to modern surveillance studies, self-interest has, for instance, been invoked in proposed explanations of the privacy paradox. Several popular explanations of why people seem to behave online as if their privacy were not important to them, while at the same time reporting that their privacy *is* important to them, appeal to a self-interested cost-benefit analysis (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017).

[3] It is standard, when introducing ethical theories, to include a third kind of theory, namely, virtue ethics. However, virtue ethical theories are not straightforwardly theories about what makes actions right or wrong, but primarily theories about what characterises a virtuous agent (and the question about which actions are right is then a question about what a fully virtuous agent would do). So, this kind of theory does not fit neatly with the discussion about what considerations may make surveillance acceptable (or right). It may be noted, though, that the discussion about deontological versus consequentialist features has a place in virtue ethics as well, as a discussion about the characteristics of the virtuous agent – to what extent such an agent displays consequentialist and deontological thinking, respectively.

[4] Some versions of consequentialism consider outcomes indirectly: Instead of assessing the value of the outcome of an action directly, they assess the value of the outcome of applying or internalising principles, rules, dispositions, or the like, that recommend or result in the action. In the context of online surveillance, a consequentialist may consider either the consequences of a particular instance of surveillance directly, or, for instance, the consequences of a certain surveillance practice (of an actor). This difference is not important to my discussion in this chapter.

[5] There is, of course, a risk that those who voluntarily choose to participate in a questionnaire survey generally share some characteristics that may affect the responses. In relation to this worry, it is important to (again) note that I do not claim to say anything about other people than precisely those who answered the questionnaire. However, it could also be noted that there is already a selection made regarding which group the survey addresses: young students with considerable digital experience, who spend a large part of their time online. We can expect there to be a general interest among this group in the kind of questions addressed in our survey, and thus, quite a large interest to participate irrespective of one's particular views on the different questions asked. One student group of 90 persons (a subgroup of the total group of respondents) was invited to answer the survey directly in the classroom at the end of a lecture. The teacher left the students and there was no way for the teacher to check if any particular student answered. In this group, the response rate turned out to be close to 100 per cent. Interestingly, the response patterns in this subgroup are generally very similar (for the questions tracking the respondents' attitudes, behaviours, beliefs, views, or opinions) to those in the total group.

CHAPTER 7

Smartphone privacy

Finnish young people's perceptions of privacy regarding data collected when using their mobile devices

LIISA A. MÄKINEN & JOHANNA JUNNILA

DEPARTMENT OF GEOGRAPHY AND GEOLOGY, UNIVERSITY OF TURKU, FINLAND

ABSTRACT

In this chapter, we explore Finnish teenagers' experiences and understandings of privacy concerning the data stored in and flowing through their smartphones. Building mostly on qualitative interview data collected in Finland, we investigate what kind of factors are meaningful for young people when thinking about privacy on mobile devices, and how the level and nature of privacy required depends on the audience. Our results reveal that banking information, passwords, fingerprints, and locations were considered the most private information on smartphones. A myriad of personal factors affected how certain information was deemed more private than other kinds, hinting that much of this judgement lies in the context. Privacy matters to young people, but it seems to hold more meaning in social contexts and often remains overlooked in institutional settings, where the potential risks of privacy losses may seem unclear, abstract, or even irrelevant.

KEYWORDS: privacy attitudes, smartphones, applications, tracking, teenagers

Mäkinen, L. A., & Junnila, J. (2023). Smartphone privacy: Finnish young people's perceptions of privacy regarding data collected when using their mobile devices. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 145–166). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-7

Introduction

Young people spend much of their waking hours on their smartphones and online. In Finland, 99 per cent of people aged 16 to 24 use the Internet on a daily or almost daily basis, and 98 per cent use it on their smartphone (Statistics Finland, 2021). During the 2000s, the mobile phone became "woven into the fabric" of young people's lives as a source of entertainment, a creator of social stimuli, and an aid to escapism (Grant & O'Donohoe, 2007: 232). Contemporary smartphones are used for communication, social media activities, creating and consuming media, playing, reading, navigating, shopping, studying, monitoring health, and seeking information. They allow children and young people to communicate privately with their friends, explore different identities, and learn social skills independently. As such, smartphones can be "tool[s] for autonomy and freedom" (Vickery, 2015: 284), but they are simultaneously collecting vast amounts of data regarding these personal communications, daily activities, and social contacts. Indeed, while smartphones may bring young people certain freedoms in communication and mobility, they can also be used by parents to monitor and supervise their children's behaviour (Barron, 2014; Oostveen, 2014; Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021).

How children and young people use their mobile phones has been the focus of much sociological research over the last few years. Topics have included parental surveillance practices (Barron, 2014; Devitt & Roker, 2009; Fotel & Thomsen, 2003; Oostveen, 2014; Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021; Williams & Williams, 2005; Wisniewski et al., 2022); texting and sexting[1] (Grant & O'Donohoe, 2007; Hasinoff & Shepherd, 2014); and targeted advertising (Chen & Wen, 2022) (for other examples of highly cited articles relating to young people and mobile phones, see Yan, 2018). Research on this topic is complicated by the fact that the phenomenon is often analysed not as a separate subject, but as part of a bigger whole. This bigger concept of a media ecology, with smartphones often at its centre, describes how traditional and digital forms of media are now often combined for a variety of purposes (Ito et al., 2008; Vickery, 2015; Wisniewski et al., 2022). Consequently, much of the research on how young people communicate online is also relevant to the present study.

It is nevertheless surprising that only a few researchers have focused on privacy in the context of mobile phones and young people; these studies have focused either on how they communicate on their smartphones, or more recently, on location-tracking technology. For example, Ian Grant and Stephanie O'Donohoe (2007: 236) analysed perceptions of texting in their research on young people's motivations for using a mobile phone, arguing that young people see their smartphones as a "private form of communication". Similarly, but in a more specific context, Amy Adele Hasinoff and Tamara Shepherd (2014) found some widely accepted and shared norms for privacy in sexting. Meanwhile, in 2015, Jacqueline Ryan Vickery based her ethnographic research on the social privacy challenges facing young people from low-income and non-dominant social backgrounds, concluding that they negotiate and manage their privacy by developing various deliberate strategies to resist social convergence and adult- and peer-surveillance. While context-specific, these studies show certain commonalities and indicate how mobile-device privacy is important even in challenging circumstances. More recently, privacy has become a relevant frame in research examining family use of location-tracking apps on mobile phones, in terms of how location tracking is perceived, used, negotiated, and resisted by parents and young people alike (Sukk & Siibak, 2021; Widmer & Albrechtslund, 2021).

While these studies provide important insights into young people's perceptions of privacy in the mobile context, none take into consideration the vast scope of data that such devices store and share. As well as storing details of one's location and private communications, mobile devices (and the apps on them) store contacts, photos, videos, recordings, passwords, banking information, social media interactions, information on the surroundings of the device, and biometric data – all of which is directly traceable to the user. Each smartphone has a unique ID distinguishing it from others which cannot customarily be disabled by the user. This ID can be used, for example, by a manufacturer or service provider to collect data on the calls and messages made, and this also counts for the installed apps. Before installing an app, the user is usually required to give their permission for it to access certain information on the smartphone. This information will concern use of the app, but may also include contacts, call logs, schedules, location data, or Internet data, which can then be sold by the app provider to third parties. As data is collected by multiple actors and stored in various locations, it is often difficult or impossible to ascertain exactly where one's data is stored, who has access to it, and to whom it might be sold in the future (Aditya et al., 2014; Furini et al., 2020, Ketelaar & van Balen, 2018; Martin & Shilton, 2016; Sipior et al., 2014).

Thus, privacy is particularly pertinent in the smartphone context due to the many layers of data collection and the number of actors involved. In this chapter, we analyse qualitative data gathered from young people in Finland about how they define privacy and its limits in the mobile context. Our work was guided by two main research questions: 1) what information do young people consider to be most private or personally sensitive to them on their smartphones; and 2) who are the people they want to share that information with, or hide it from? The rest of this chapter is structured as follows: first, a brief introduction to existing privacy research, especially regarding young people's views on it; then, a presentation of our data and methods, followed by a detailed analysis of the two research questions; then, our results in the context of existing research; and finally, our conclusions.

Briefly on privacy

Although extensive research on privacy dates back at least a century, controversy still surrounds its precise definition. Focusing on the aspect of information control, one definition is that privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967: 5). Understood this way, privacy focuses on the individual, and is a means for reinforcing individuality (Bennett, 2011). Another classic definition of privacy focuses on its social value, arguing that privacy is "an interpersonal boundary control process" (Altman, 1976: 27). The boundary is one between "closedness and openness" and, rather than being fixed, is negotiated through social practices (Steeves & Regan, 2014: 303). In this respect, privacy acts as a means for creating and maintaining social relationships, determining the nexus, or balancing point, between the need to withhold personal information (in some contexts) and the need to divulge it (in others). As such, privacy is often perceived as a trade-off in which the benefits of sharing are weighed against any possible negative repercussions – this is often referred to as privacy calculus (Baruh & Popescu, 2017; Marwick & Hargittai, 2018; Steeves & Regan, 2014; Vickery, 2015).

The context of where information sharing takes place is perhaps the most important factor in analysing issues of privacy. To this end, Helen Nissenbaum (2004, 2010) has suggested a framework for determining the contextual integrity of privacy. She argued that in any context or sphere, there are two types of informational norms which apply: "norms of appropriateness", which deem what is appropriate to reveal; and "norms of flow or distribution", which deem who this information should be shared with (Nissenbaum, 2004). Privacy is thus greatly affected by the kinds of social norms applied. This also manifests itself in the way some forms of surveillance might go unproblematised in certain contexts but provoke criticism in others. Nissenbaum's contextuality framework is thus a useful tool for analysing young people's privacy attitudes and strategies, as they communicate with a multitude of different audiences on a variety of platforms, many of which are online. These are complex to analyse, however, as online environments consist of different, overlapping contexts, some of which may be combined with offline relationships to varying extents, depending on the platform. These overlapping contexts and the ways in which performances flow between them also complicate online privacy (Steeves & Regan, 2014). Meanwhile, smartphones complicate the situation further; in addition to information flowing between various online environments, data and metadata are also often collected without the user's knowledge and sent to locations unknown to them. Smartphones are used in contexts where risks are perceived and accepted differently, depending on the social norms and what is known or presumed about the flow of data.

In addition to this contextual value, Valerie Steeves and Priscilla Regan (2014) argued that privacy has performative, dialectical, and relational value for young people too. Performative value comes from the need to have a private or safe space to explore identities. Dialectical value comes from the need to find balance between public and private needs through constant negotiation. And relational value emphasises the need for reciprocity in any social relationship when sharing information. If it is only shared unilaterally, the relationship is instrumental and can only ever be, at most, consent-based. Consent is founded on the idea that organisations notify users about their information policy, and users make informed decisions based on that; this is seen to protect privacy. This approach, however, has only a narrow understanding of what the lived realities of privacy are, and there have been many critiques of the privacy self-management paradigm, especially in the face of expanding algorithmic surveillance and the use of Big Data (e.g., Baruh & Popescu, 2017; Lehtiniemi & Kortesniemi, 2017; Steeves & Regan, 2014; Solove, 2013).

Steeves and Regan's (2014) typology of the various social values of privacy demonstrates concrete ways in which young people negotiate their privacy online, and it also offers tools for contextualising how young people experience privacy. Youth researchers generally agree that young people *do* care about their privacy, and while privacy may be contextual and networked, it has not lost its meaning for teenagers in the social media era (boyd, 2014; boyd & Hargittai, 2010; Cocq et al., 2020; Livingstone, 2008; Marwick & boyd, 2014; Marwick & Hargittai, 2018; Steeves & Regan, 2014; Stoilova et al., 2020; Vickery, 2015; Wisniewski et al., 2022). Although privacy management may indeed be difficult, young people have several ways to micromanage their online practices on a day-to-day basis. Without wanting to hide "anything 'bad'", they still want to "control the context in which information is disclosed and shared, as well as to control access to their digital identities, spaces, and devices" (Vickery, 2015: 281–282; see also Cocq et al., 2020; Marwick & Hargittai, 2018; Wisniewski et al., 2022).

In recent decades, research has duly recognised the magnitude and complexity of surveillance for everyone – not just young people. However, a more precise analysis of particular age groups – and their personal or individual experiences of being monitored in different surroundings and contexts – is still needed. Research on the relationship of children and teenagers to privacy increased in the 2010s, but the focus has so far generally been on interpersonal contexts rather than organisational and commercial contexts, where data is not so much actively given out as automatically harvested (Stoilova et al., 2020).

We recognise that in analysing how surveillance is felt and perceived on an individual level, many surveillance scholars have argued that privacy is an inadequate concept (Ball, 2009; Bennett, 2008; Gilliom, 2001). Nevertheless, in the context of this research, it offers a valid conceptual tool for analysing different levels of data collection, various data items, and the complex perceptions that young people have towards these issues. While recognising the challenges of investigating surveillance in the context of privacy, we also see that privacy remains an important "way to frame the contemporary problem, as a regime of governance and as a set of practices" (Bennett, 2011: 486).

To summarise, online environments (including smartphones) are complex surroundings from a privacy perspective. They enable young people to create, develop, and test their identities, but at the same time, they are subjected to vast amounts of visible and invisible monitoring from their peers, commercial actors, and government organisations (Regan & Steeves, 2010; Steeves & Regan, 2014). As smartphones are primarily used for online activities, their use should also be analysed as a complex web of displaying information for some while hiding it from others, and for managing not just audiences, but also one's own actions. Simultaneously, it is important to bear in mind that young people and (adult) society may well have different understandings of "the social contexts in which teens disclose information, perform identity, and communicate with one another" (Vickery, 2015: 282; see also Herring, 2008). To get a better idea, then, of precisely how information is shared between people, organisations, and these various social contexts, we must ask young people themselves.

Data and methodology

The data for this research was collected in Finland between March 2020 and December 2021 as part of a larger research project examining the subjective experiences of surveillance. The participants were recruited through schools, municipalities, and nongovernmental organisations in two large Finnish cities. Altogether, 37 people aged 12 to 19 participated in this research: 24 of them were girls, 10 boys, and 3 identified as other or did not reveal their gender. The data collection used a mixed-methods approach combining concept mapping, Q-sorting, and in-depth interviews; not all participants took part in all three data collection methods. This chapter uses all the data collected from all 37 participants but pays closest attention to the qualitative interviews conducted with 14 of the participants. The overall data collection process, its methodological framework, and the size of each dataset are described below.

The data collection in its entirety was built on a 51-item list entitled "What my phone knows about me".[2] The list included items such as basic information (e.g., name, age, occupation); contact information (mobile phone number, e-mail, home and work addresses); online communications and social activities (e.g., the content of messages sent and received, a list of the words used in messages); metadata (e.g., where and when messages were sent and received, where each photo was taken, how often each app was used); location data (e.g., current location of the smartphone, information about regularly visited locations and usual routes); biometrics; content stored on the smartphone (such as documents, photos, and recordings made on it, downloaded to it, or uploaded from it); items relating to what the smartphone can "see" or "hear" with its microphone or camera; details about purchases made on the smartphone; banking and credit card information; and passwords.

Data collection began with a concept-mapping exercise, where participants were asked to rate each item listed on a 1–5 scale according to how sensitive or private they considered it. Participants were also asked to rate each item based on how comfortable they would feel revealing that information to three separate groups: people close to them, people they knew in their community, and people or organisations they did not know. Concept mapping, as a participatory qualitative research method, was originally developed by William M. K. Trochim (1985) as a means of using quantitative data to provide "structure and objectivity to qualitative data" (Burke et al. 2006: 1393). An online version of this method was used via the GroupWisdom™ site, with 30 participants.

Next, we conducted semi-structured qualitative interviews with 14 participants (11 girls, 2 boys, 1 other), who were all aged between 15 and 19. We conducted four interviews of which two were in person (with one researcher participating face-to-face and one remotely) and two, due to the Covid-19 pandemic, fully remote via Zoom. One interviewee was met one-on-one, while the rest participated in focus group interviews. The interviews each lasted 60–95 minutes (average 80), with a combined length of 5 hours and 20 minutes. The discussions were then transcribed, resulting in 111 pages of data. The interviews began with a Q-sorting exercise. Like concept mapping, Q-sorting is a three-step method – participants firstly rank a set of items on a fixed rating scale, and then the rankings undergo quantitative and qualitative analysis (for more on methodological issues, see, e.g., Rost, 2021). In this Q-sorting task, participants ranked the same 51-item list used in the concept-mapping exercise. They began by choosing three items that described topics they considered to be the most sensitive or private, and then three that were the least. After that, they chose four of each, then six, and finally, eight. An online platform called Miro (www.miro.org) was used for the task when it was done remotely, and small cards were used in the face-to-face meetings. This resulted in 13 Q-sorting tables being returned, which, along with the concept-mapping tasks, could then be discussed in the interviews. Additionally, the interviews focused on three broad themes: 1) privacy in general (e.g., what it is, how it is defined, its value, reasons for privacy, and the consequences of privacy invasions); 2) privacy as a contextual process (who they want privacy from); and 3) privacy in the specific context of one's mobile phone (e.g., whether the participants think about surveillance and data collection when using their smartphones or manage their privacy settings somehow).

The interviews were analysed using data-driven, qualitative content analysis focusing on the specific research questions and building on replies received from the Q-sorting task. Content analysis is a common and flexible method of analysis for many different types of qualitative data. It can be used on its own or in combination with, for example, discursive or thematic analysis, and allows the data to be quantified to some extent, even if no actual statistical correlations are sought (Prior, 2020). The interviews were analysed using NVivo-software, and the quotes in this article were translated by the authors after the analysis. Pseudonyms have been used throughout for all the participants.

The quantitative methods – particularly the Q-sorting task – offer a backdrop for the descriptions of how young people perceive private information. However, the focus of this chapter is on the qualitative interviews and achieving a deeper understanding through their in-depth analysis. While the number of participants is small – meaning the results are not generalisable to those of a similar age in Finland (let alone globally) – they do shed light on the kinds of views and experiences young people have about smartphone privacy in the 2020s. The study was also reviewed and approved by the Ethics Committee of the University of Turku. In the next two sections of the chapter, we first examine which items our participants considered most private to them and their thoughts on why, then we analyse the different audiences envisioned by them – in particular, those they wanted to hide information from. Following these two analysis sections, our results are then discussed in a wider context and some conclusions drawn.

Young people's perspectives on privacy concerning specific data items stored on their smartphones

Of all the information stored on their smartphones and apps, respondents considered credit card and banking information to be the most private. In the Q-sorting task, credit card and banking information was chosen by 12 of the 13 as one of the three items most private or sensitive to them personally, and in the concept mapping it was given a rating of five (extremely sensitive or private) by all respondents (*N* = 30). Credit card and banking information were thus considered very private, as they concerned money and were thought of as information belonging to no one else. As one of the interviewees, Iris (aged 19) said: "Then there's my banking information. I'd prefer not to have it as public information, because it's my money and it doesn't concern anyone else". In addition to concerns of losing their money, the respondents also worried that someone could gain access to other private information using this data: "With banking information", Oliver (aged 15) observed, "you can gain access to someone's health records, which can be sensitive, or someone might think they are".

The passwords on a mobile phone were the next most often mentioned: seven participants chose them as one of the three most private pieces of information (with an average rating of 4.50 from the concept mapping respondents). The issue of passwords also revealed some ways in which young people aimed to manage and protect their privacy: "I put strong passwords on my phone so that nobody can get information from it", noted Alva (aged 17), and "I also save all my passwords on paper. I write them down so that I don't have them anywhere digital".

The fact that credit card and banking information and passwords were chosen as the most private or sensitive data by so many respondents shows a somewhat technically oriented and formal approach to privacy and a very tangible understanding of the kinds of risk associated with access to finances or other sensitive information protected by this data.

The third choice varied more, but fingerprints were among the most frequent (three mentions and an average rating of 3.87). In terms of content, fingerprints are closely attached to the two former items, because like passwords, and to some extent banking information, they can be interpreted as a means of accessing other information: gateways to something *more* valuable. Rosa (aged 16), for example, stated that "with [my] fingerprints, you can get into my phone […] and my phone has all the information you've listed here".

In addition to fingerprints, the item list included two other biometric details: "what my face looks like" and "what my voice sounds like". Face and voice, however, were not seen as being nearly as sensitive forms of information as fingerprints. Indeed, most participants ranked them as "not at all sensitive or private" to them. The interviews revealed that the potential uses of biometric recognition were unclear to many respondents:

> And then, of course, my fingerprints, because I don't want to be framed for a crime [laughs] […]. It sounds far-fetched, but couldn't they actually do it? I mean, like, murder someone and put my fingerprints there, and then it's my fault? (Kris, aged 16)

> Julia: But this is also a bit double-edged, "what my voice sounds like"; what if someone takes my voice and does something with it?
> Sara: But what would they do with your voice?
> Julia: I don't know.
> Kris: […] I mean, nowadays you can do anything.
> (Sara & Julia, aged 15; Kris, aged 16)

> Rosa: Is my face private?
> Sara: No, I can see your face [laughs].
> Kris: It's a little private because you have, for instance, Face ID.
> Sara: Yeah, but…
> Zelda: Even if you had a picture of Rosa, you couldn't get into her phone.
> Kris: Couldn't I?
> Everyone else: No!

> Rosa: You'd need… like a 3D […]?
> Sara: But where would you get a 3D image of Rosa […]?
> Kris: I wouldn't, but someone could.
> (Kris, Rosa, & Zelda, aged 16; Sara & Julia, aged 15)

The above quotes show how the respondents ponder what might be done with their voice or an image of their face, but because they do not know, they end up not choosing these as being some of their most private information. We witnessed similar confusion around other items on the list, such as "the phone's unique device ID number" – in almost all interviews, the participants asked what it actually meant.

The last item on many respondents' list of three was either something relating to location (altogether eight mentions for five different items) or something relating to personal content stored on the smartphone (a total of seven mentions for three different items). Participants thought the idea of someone they did not know being able to track their location to be "scary", "disturbing", "annoying", or "plain creepy". For example, Rosa (aged 16) explained that "it's a little disturbing if someone knows precisely what time you go to school and which way you go there and so on". Similarly, Mia (aged 16) explained that she chose "my direction and speed of movement" as one of the most sensitive pieces of information, arguing that "if someone knows that, then they also know my location, and it's quite a serious security risk". Location data was also seen as necessary to protect for personal reasons, such as going to the doctor's office, or not wanting to reveal who one is spending time with.

When moving on to the next four most private or sensitive items, information concerning location was chosen more regularly, cited altogether 18 times (across seven different items), with the single most often mentioned of these being home address (eight times). This seems particularly interesting, as in Finland, people's home address is quite easy to get from public registers: Anyone can find out where anyone else lives with a single SMS or a call, unless the person in question has specifically denied access to that information. Home address was linked to security issues and feeling safe in one's own home. Sara (aged 15), for example, talked of her home needing to be "like your own place where you'd want to be safe, and you wouldn't like if everyone knew where you lived and could come there".

One item particularly worthy of mention here, because it provoked quite different responses – exemplifying how perceptions of privacy can vary wildly – was gender. Most respondents were completely indifferent to it, considering it one of the most public pieces of information. For example, when Kris (aged 16) was asked about the items they felt least sensitive about on the list, they replied, "my name, age, and gender, they are things I could tell anyone the moment I meet them". However, our dataset included some respondents who had non-binary thoughts about their gender or did not want to reveal it. For some of these participants, gender was therefore a more sensitive issue and private information. The difference between Kris's response above and Nova's response below is striking in this respect, highlighting just how contextual privacy is – not only in terms of who is telling what to whom, and in which particular situation, but also because the same issues may have completely different meanings for different people:

> Well, my gender is like... I wouldn't say, somehow, I wouldn't say that I'm a woman, but I wouldn't go as far as to say non-binary. So, because of that, it's a really sensitive subject for me, and I would like to keep it secret. [...] I don't know, I feel like everyone is labelling [each other], and I can't really talk about these things very publicly. [...] So because of that it's a bit more of a private issue. (Nova, aged 18)

Young people's considerations of privacy in terms of which specific audiences can access their data

There were some variations in how young people viewed the data stored on their mobile phone, and who they felt comfortable about being able to access it. In other words, we were asking them what they thought about privacy in terms of sharing data with specific audiences. Participants also gave their own unprompted examples of such audiences, their own definitions of what privacy means, what makes something private, and how privacy can be violated. Specific audiences cited by the participants included unknown people, acquaintances, ethnoreligious communities, friends, relatives, family members, and just themselves. Some references were made to partners, authorities, or organisations – but they were surprisingly few. Below, we consider these different audiences one by one, proceeding from wider or unknown audiences towards people closer to the participants, and then to institutions. We conclude by connecting these audiences to participants' notions of the differences between online and offline environments.

Thinking about an unspecified "someone" or "everyone" provided the general baseline for participants – the "gut feeling" of privacy, per item. Alva (aged 17), for example, said "I'd like to have privacy from anyone whose name I don't know – that's like a good basis for me. Usually, if I know someone's name, I know that person at least to some extent". Groups of unfamiliar people with slightly different nuances were also mentioned by participants: people whose names they did not recognise, or they did not know but their friends did, and foreign people (insofar as it came as a privacy violation from someone abroad). There were also certain information participants did not want to share with anyone else, either because it was extremely intimate or just for the joy of being able to do something without anyone asking questions:

> As a rule, you may just want to feel that you can keep some things to yourself. That you don't have to worry that some things about you will get spread about without you having any control over it. So, in that way, [I want privacy] from everyone. (Iida, aged 17)

A connection with someone of some kind usually made sharing information feel more natural. Indeed, some participants referred to privacy in terms of trust. They wanted people close to them to respect their privacy, explaining that this meant they could trust that their personal matters were safe with these people. In this respect, private information was seen as something that is not fully exclusive yet expected to stay within only a small circle. However, other participants felt more at ease revealing something to complete strangers – for example, issues that were personal to them but that they knew someone already in their lives would not understand or appreciate. Relationship status was one such issue: For some, it felt more comfortable to share this with complete strangers, as then it was less likely to reach people closer to them whom it might upset.

Interestingly, it was the acquaintances that participants knew partly but not closely that some wanted privacy from the most – people with whom they did not have any really meaningful relationship or mutual trust, yet from whom they also lacked comfortable anonymity:

> The people you don't know that well but who you meet occasionally, like acquaintances, are maybe the worst. I mean, you know you'll meet them again sometime, but you don't really know them. If they were just someone you'll never meet again, it would not feel so difficult. (Maria, aged 16)

This might partly explain the popularity of anonymous apps, such as Jodel, which many of the participants used. According to them, its anonymity provided a suitable place to ask "stupid questions" that they might otherwise have never dared ask. However, it was also a location where bullying and trolling were rather common, and it became apparent that Jodel was a place of only partial anonymity, as it blended online and offline life, since many schools had their own channels on the app.

In terms of family, relationships with parents were closer for some participants than for others, but most required some modicum of privacy:

> [You do want some privacy] also from your family, especially at this age, you need your own space and so on. Your family doesn't have to know everything that's going on in your life. I also feel it's good to keep some things just to yourself [...]. You don't have to always share everything. (Sara, aged 15)

In some cases, this desire for privacy also made some participants approach their parents about it and consider decreasing the number of digital traces they left behind. With some amusement, Zelda (aged 16) explained how she found out her father could track her whereabouts during the school day by monitoring her purchases: "I was just surprised [that my father could see where and when I'd been using my bank card]. Then I was just like 'okay, in certain situations, I'm just going to have to use cash'". Indeed, most of the participants had their own smartphone already as younger children, so they were used to parental controls, mobile-enabled tracking, and negotiating with parents about smartphone use. However, as they had become teenagers, parental attempts to control their activities had decreased or changed in form – parents were usually more concerned about the length of time spent on screens rather than what they were doing on them:

> For ages I had one of those screen time apps, where you could see what apps I use, for how long, and how long I'm allowed to use them [...]. Now I'm about to turn 18, so they don't follow it that much anymore. (Camilla, aged 17)
>
> One thing that really annoyed me was they wanted to know my location all the time. [...] I feel old enough now to take care of my own whereabouts, and I always tell them where I am, but they still wanted to know it. [...] But then we talked about it and decided that they don't have to track it. (Rosa, aged 16)

Location tracking was not a simple issue, however. While participants generally wanted some privacy about their location, they also felt that sharing it with family or other people they trusted was sometimes a useful safety measure, actively sought from parents, or in some cases even close friends, when this feature might also serve social purposes – such as planning gatherings:

> My parents have never wanted to track my location or anything. When I was younger, I probably wouldn't have wanted to let them know, but just recently, when I said "hey, I've put [my location] on now so you can see where I am if someone tries to kidnap me", my parents were a bit like "why should we know where you are?" And I was like "well... because I want it!" (Kris, aged 16)
>
> Iida: I don't have anything like that [location tracking] with my parents, but I do have with my friends. [...] If one of us goes missing or something happens, we know where they are. [...] It was our mutual decision, so that if someone needs help or their phone dies, you can know exactly where they are. [...]
>
> Interviewer: So, it's ok to check and see where your friend is right now?
>
> Iida: [Yes.] We also use it, for example, if we are going to meet, to check when the others are leaving [home]. None of us is usually late or too early because everyone knows where everyone else is. (Iida, aged 17)

When asked to think about different forms of institutional surveillance, most participants expressed trust in the Finnish authorities and thought that their data was safe with them, referring to how authorities are obliged by law and employment contracts to respect confidentiality. For example, Leo (aged 15), explained how this type of organisational surveillance is “not that big a problem, if they use the data responsibly, so the police are not giving it out”. Trusting the authorities with personal information meant one could expect “proper privacy” – as one participant put it:

> In that way, it’s easy to disclose [information] to them because they’re... bound by professional confidentiality. I trust that my data stays safe, because it’s [written] in their employment contract, after all. When they got the employment contract, they signed it and agreed to it, so then I trust it too. (Iris, aged 19)

However, some participants had quite a different opinion: Some referred to leaks and other mishandlings of personal data that have happened and diminished their trust in organisations and authorities. “To be honest”, admitted Nova (aged 18), for example, “I don’t trust [authorities or organisations]. I’ve seen so much news about e-mails getting leaked, that to my mind, it’s very alarming. I mean, you just can’t tell... anyone could do it, so no, I don’t trust [them] that much”. Some participants were therefore strongly against organisations and commercial entities gathering and selling their data for profit, sometimes comparing different companies by the reputation they had in managing their customers’ data. Others did not find it quite as problematic, focusing on the benefits of customised advertising, or else they saw data collection as something that all companies must do. Most participants, however, had no strong opinions one way or the other.

The discussion about different audiences tended to focus on possible privacy violations: Participants considered both the nature of shared information and possible consequences of privacy breaches when deciding whom to trust with their information. However, in social contexts, privacy violations were not seen in black-and-white terms; they were considered less severe if they happened by accident or stemmed from good intentions, such as caring about someone’s well-being. As for institutional surveillance, participants also referred to the trade-offs needed to operate in the smartphone culture of today, where participation without giving away personal information is increasingly difficult. Some participants also thought that since their personal data was only the tiniest fraction of a much bigger mass of data, it was largely irrelevant. Regardless of the exact audience, however, many participants felt it was disturbing that people could make decisions based on knowing things about them; especially when it was information they did not realise was being collected in the first place, could not access themselves, or that came from many sources. “It’s a bit scary”, observed Kris (aged 16). “If you look at this... 'a list of the words I use in text messages and e-mails', not even I have any idea what they could be".

Participants referred to situations where they actively managed their different audiences by making decisions about privacy or sharing based on trust, previous experiences, or other factors. Technical measures were considered important too, especially when travelling abroad, as one could not be so sure of the situation as at home:

> I protect my device when using a public network. If someone breaks into that public network, at least my data won't be stolen. There are some skilful hackers and such [...]. Maybe not that many in Finland, but if I go abroad, I protect myself. (Iris, aged 19)

However, other people were not just seen as potential audiences for leaked private information, they were also seen as individuals who themselves have their own expectations of privacy. For many participants, other people's privacy was very important, and some were even in positions of trust themselves (e.g., at school or in politics). This meant they handled information regarding others and needed to take care, especially with contact information and messages. "Messages and calls, well, they are not exactly private as such", remarked Nova (aged 18), for example, "but [...] some people might come to me with things they don't want other people to know about. That's why I am careful, too".

All the participants considered the norms and issues governing privacy online and offline to be quite different. Managing information online felt significantly more difficult, to the point that offline information seemed far less of a problem to manage that any information spreading online. For example, Oliver (aged 15) explained:

> In "real life", if you don't tell anyone anything sensitive about yourself, then in principle it can't spread, whereas online, someone can just dig up all the information [you might not have filtered] from your profile, without you being able to do anything.

Other differences which made information management online more difficult than offline was the speed with which information could spread, how such audiences could be much wider and unknown, and that screenshots could be taken of private conversations as damaging "proof".

> You're much more vulnerable [online] to privacy violations, since you are more in control of what you tell others [offline]. For instance, if you tell a friend something, that friend can't share that so easily. But if you send a message, it stays there, and it's much easier to share. (Sara, aged 15)

However, it was also noted how it is possible to decide whether you show your face or name online, while in public, these are more difficult to keep private. The Covid-19 pandemic has brought some interesting nuances to this distinction, though, now that using a face mask in public has become quite commonplace and many traditional face-to-face events and concrete environments, such as schools, have at least temporarily moved to being done remotely online.

In conclusion, participants recognised various kinds of audiences and degrees of privacy which distinguished these audiences. In general, they felt more comfortable sharing information with people closest to them, but sometimes anonymity encouraged openness and was also considered a safe place to share personal issues. Lastly, most of the participants trusted their data with national authorities, but opinions were divided when it came to private organisations using and selling it.

Discussion

Through analysing young people's perspectives on smartphone privacy, we found that participants most often referred to items of a more technical and formal nature (i.e., banking information, passwords, and fingerprints), which, if leaked, would have the most directly tangible effects (e.g., financial losses). These data items were generally felt to be easier to control compared to, for example, the continuous and hidden accumulation of message or location data. While the need for privacy can be seen as a desire to protect "both tangible and intangible properties" (Furini et al., 2020: 1055), tangible information is more likely to be easier to recognise and protect. It is also worth noting that, although some data items are considered sensitive regardless of the context in which they are shared, there are also certain contexts which are consistently more sensitive than others. Banking, for instance, is one such context where privacy has always been found to be important (see, e.g., Martin & Shilton, 2016). Choosing to engage in any kind of financial transaction online, particularly via a mobile device such as a smartphone, is thus often preceded by careful consideration of the trustworthiness of the site (Marwick & Hargittai, 2018). This technical data with tangible effects can also be understood as a kind of liminal form of information because it also acts as a gate through which other information or vulnerable online spaces can be accessed. In Finland, online banking details are used as secure login data for online sites and services in many areas (e.g., social security, welfare, healthcare, taxes, electricity, and insurance), so losing that data could lead to a lot more than just financial losses.

Overall, our data revealed that the concrete risks of privacy breaches, such as physical safety, were of most concern to participants, with the consequence that online risks were often overlooked, unless they, too, had physical consequences – particularly in cases where location data was compromised. These results perhaps reflect what is taught in schools about privacy online, where the focus of e-safety is on the concrete threats of hoaxes and predators. This would also explain the often quite shallow understanding many young people displayed of the extent of institutional surveillance and data collected about them – and its potential consequences. Young people have rarely had any experience of privacy violations committed by an institution that might affect data sharing (Marwick & Hargittai, 2018; Stoilova et al., 2020).

While our participants' focus was on real-life risks, their expectations for privacy differed in online and offline contexts, and they decided what information they wanted to share, how, and to whom, depending on whether the context was online or offline. We argued above that privacy can be seen as "an interpersonal boundary control process" (Altman, 1976: 27), where the boundary between what is shared, where it is shared, and how it is shared, is constantly negotiated. The context where this negotiation takes place affects and is affected by individual privacy expectations. Examining privacy as a contextual process might seem inevitably difficult, as contexts are negotiated and fluid. However, previous research has proven that people's privacy concerns are *predictably* contextual and that it is possible to measure "nuanced, contextual concerns" and decipher which data types are sensitive in which contexts (Martin & Shilton, 2016: 211). Indeed, while the participants in our study had varied notions of audiences and the privacy of certain data items, there were some ideas shared by all.

We must bear in mind, however, that the context for sharing information via a smartphone is somewhat nebulous, as it will inevitably be leaked to more audiences than just the intended. The actions of smartphone users leave unintentional traces, which often makes it harder to manage privacy as one might like (see also Hasinoff & Shepherd, 2014; Steeves & Regan, 2014; Stoilova et al., 2020). Because of this difficulty, young people will control what they can – for example, access to the more technical, clearly defined data – or focus on the visible and intended audiences and disregard those which remain unseen (i.e., system-level data collection).

It has been argued that the audience matters as much as the information itself; that defining privacy should not be "tied to the disclosure of certain types of information, rather a definition centred on having control over who knows what about you" (Livingstone, 2008: 404; see also Livingstone, 2006). However, while this argument is pertinent to various social groups, it overlooks much of the institutional context of surveillance – as the young people in our study also seemed to do. Issues of privacy in social situations were dwelt on more than institutional types of surveillance. While the typical risks of system-level data collection were recognised – data exploitation, data loss, and data overreach (e.g., Aditya et al., 2014) – they were more an afterthought, barely affecting how information is shared between social groups.

In conclusion, we would argue that, rather than young people being unaware of the potential privacy risks they are taking, they are making a conscious choice – knowing full well it is one they cannot avoid. They understand and recognise (some) of the potential risks, but choose to not dwell on them, as doing so might prevent them from continuing to use their device (see also Marwick & Hargittai, 2018). So, if an individual really wants to address privacy issues in smartphone culture, it might mean not participating in it at all.

Yan (2018) has argued that the modern mobile phone has two core features: personalisation (as it aims to satisfy the individual user's needs) and multifunctionality (integrating features from other technologies and adding new ones). After examining how contemporary youths use their smartphones, two more core features become prominent: the phone's proximity to the user (as it is usually kept "within arm's reach") and its perpetual activity (as the phone is nearly always on and in almost constant use). These four features have strong links to questions of surveillance and privacy and resonate with our research findings.

As smartphones aim to satisfy all kinds of individual needs – be they physical, social, cognitive, or emotional (Yan, 2018) – it becomes useful for phone manufacturers and service and app providers to predict those needs. Thus, it is necessary to collect all kinds of data to create individual (consumer) profiles, which can then be used for the direct marketing of new services and apps. The aim of surveillance, then, is to sort people into categories for which services can be provided, turning surveillance into a form of social (and economic) sorting (Lyon, 2003). The fact that the smartphone fulfils one's specific needs makes any trade-offs in whether to use it or not trickier – it is difficult to reject a technology when it can bring so much personalised pleasure.

The multifunctionality of the smartphone means that the collection and storage of information may concern all kinds of daily activities – not just those connected with media use, but also other kinds of functions, from digital money (smart wallets, mobile paying) to measuring bodily activities (biosensors, self-monitoring apps) (Yan, 2018). Connecting many activities to phone usage that previously were quite separate increases both the volume and range of data collection and allows data to be combined and stored in an unprecedented manner. Thus, we would agree that "privacy threats from mobile devices are fundamentally different and inherently more dangerous than in prior systems" (Aditya et al., 2014: 7).

Furthermore, the phone's proximity to its user (see also Vickery, 2015) adds a deeper layer to this data collection, as the phone can not only collect biometric and location data on its user, but also "listen to" and "watch" them. Thus, in addition to location, activities, and encounters, the phone can collect and store "an audio-visual record" of its user's everyday life (Aditya et al., 2014: 7). While this can be, and often is, sold to the consumer through the discourse of ease and convenience, the fact of the matter is that there can be unexpected harm related to this kind of technological embeddedness in everyday life (see, e.g., Burdon & Cohen, 2021).

When it comes to keeping the phone on all or nearly all the time, one would think that young people would be able to negotiate the boundaries of their privacy, particularly in the context of parental supervision, by arguing that they had no battery power, and hence their phone was off (see also Barron, 2014). However, to actually turn one's phone off would mean disconnecting from everything. As the phone is personal, multifunctional, always with its owner, and always on, time spent fully offline is becoming rarer and rarer. Even though life online and offline might still be considered by many – including our participants – as separate contexts, they are often present simultaneously or can leak into one another. In this respect, the smartphone operates as a liminal device combining what is online and offline at the threshold between them.

Conclusion

The majority of young people (and not just the young) use their smartphones every day and all day. Contemporary smartphones are personalised, multifunctional, and perpetually close at hand. The amount of personal data collected by them and stored in them, and the ways in which they enable and contribute to the blending of online and offline realities – especially in young people's lives – suggest that issues of privacy are more important than ever. In this chapter, we aimed to investigate how young people understood privacy in terms of the data collected via their smartphones. By examining Finnish teenagers' experiences and thoughts on the matter, we found that there are details generally considered private (such as banking information, passwords, and fingerprints), but privacy priorities depend on the context, intended audience, and personal preferences. While our data showed there was some agreement about the sensitivity of certain data items, it also proved that there were individual differences in these perceptions.

Although privacy clearly matters to young people, they contextualise potential audiences of their data in a layered manner, and social contexts seem to be more important than organisational, commercial, or institutional settings. Thus, institutional surveillance and data collection often go unnoticed or are purposefully ignored, even though they are continuously happening at the system level. This might be because these risks seem unclear or abstract, but we would argue that they are consciously ignored to enable continued smartphone use.

Acknowledgements

The data examined in this chapter was collected as part of a larger project entitled “Living within, navigating and appropriating everyday surveillance: Case studies on subjective experiences of surveillance and privacy”, funded by the Academy of Finland (SA 316013, 2018–2023). This particular study was planned in collaboration with the Canadian research project eQuality (funded by the Social Sciences and Humanities Research Council of Canada, 2015–2022).

References

Aditya, P., Bhattacharjee, B., Druschel, P., Erdelyi, V., & Lentz, M. (2014). Brave new world: Privacy risks for mobile users. *Proceedings of ACM MobiCom Workshop on Security and Privacy in Mobile Environments*, *USA,* 7–12. http://doi.org/10.1145/2646584.2646585

Altman, I. (1976). Privacy: A conceptual analysis. *Environment and Behaviour*, *8*(1), 7–29.

Ball, K. (2009). Exposure. Exploring the subject of surveillance. *Information, Communication & Society*, *12*(5), 639–657. https://doi.org/10.1080/13691180802270386

Barron, C. M. (2014). “I had no credit to ring you back”: Children’s strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance & Society*, *12*(3), 401–412. https://doi.org/10.24908/ss.v12i3.4966

Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. *New Media & Society*, *19*(4), 579–596. https://doi.org/10.1177/1461444815614001

Bennett, C. (2008). *The privacy advocates: Resisting the spread of surveillance.* MIT Press.

Bennett, C. J. (2011). In defence of privacy: The concept and the regime. *Surveillance & Society*, *8*(4), 485–496. https://doi.org/10.24908/ss.v8i4.4184

boyd, d. (2014). *It’s complicated: The social lives of networked teens.* Yale University Press. https://doi.org/10.1007/s10615-014-0512-3

boyd, d., & Hargittai, E. (2010). Facebook privacy settings: who cares? *First Monday*, *15*(8). https://journals.uic.edu/ojs/index.php/fm/article/download/3086/2589

Burdon, M., & Cohen, T. (2021). Modulation harms and the Google home. *Surveillance & Society*, *19*(2), 154–167. https://doi.org/10.24908/ss.v19i2.14299

Burke, J. G., Peak, G. L., O’Campo, P., Gielen, A. C., McDonnell, K. A., & Trochim W. M. K. (2006). An introduction to concept mapping as a participatory public health research method. *Qualitative Health Research*, *15*(10), 1392–1410. https://doi.org/10.1177/1049732305278876

Chen, Y. K., & Wen, C. R. (2022). Taiwanese university students’ smartphone use and the privacy paradox. *Comunicar: Media Education Research Journal*, (60), 61–70. https://doi.org/10.3916/C60-2019-06

Cocq, C., Gelfgren, S., Samuelsson, L., & Enbom, J. (2020). Online surveillance in a Swedish context: Between acceptance and resistance. *Nordicom Review*, *41*(2), 179–193. https://doi.org/10.2478/nor-2020-0022

Devitt, K., & Roker, D. (2009). The role of mobile phones in family communication. *Children and Society*, *23*(3), 189–202. https://doi.org/10.1111/j.1099-0860.2008.00166.x

Fotel, T., & Thomsen, T. U. (2003). The surveillance of children’s mobility. *Surveillance & Society*, *1*(4), 535–554. https://doi.org/10.24908/ss.v1i4.3335

Furini, M., Mirri, S., Prandi, C., & Montangero, M. (2020). Privacy perception when using smartphone applications. *Mobile Networks and Applications*, *25*, 1055–1061. https://doi.org/10.1007/s11036-020-01529-z

Gilliom, J. (2001). *Overseers of the poor: Surveillance, resistance, and the limits of privacy.* University of Chicago Press. https://doi.org/10.2307/3089153

Grant, I., & O’Donohoe, S. (2007). Why young consumers are not open to mobile marketing communication. *International Journal of Advertising*, *26*(2), 223–246. https://doi.org/10.1080/10803548.2007.11073008

Hasinoff, A. A., & Shepherd, T. (2014). Sexting in context: Privacy norms and expectations. *International Journal of Communication*, *8*, 2932–2955. https://ijoc.org/index.php/ijoc/article/view/2264

Herring, S. C. (2008). Questioning the generational divide: Technological exoticism and adult constructions of online youth identity. In D. Buckingham (Ed.), *Youth, identity, and digital media* (pp. 71–92). MIT Press. https://ella.sice.indiana.edu/~herring/macarthur.pdf

Ito, M., Horst, H., Bittanti, M., boyd, d., Herr-Stephenson, B., Lange, P. G., Pascoe, C. J., Robinson, L., Baumer, S., Cody, R., Mahendran, D., Martínez, K., Perkel, D., Sims, C., & Tripp, L. (2008). *Living and learning with new media: Summary of findings from the digital youth project*. The John D. and Catherine T. MacArthur Foundation Reports on Digital Media and Learning. https://library.oapen.org/bitstream/handle/20.500.12657/26078/1004007.pdf

Ketelaar, P. E., & van Balen, M. (2018). The smartphone as your follower: The role of smartphone literacy in the relation between privacy concerns, attitude and behaviour towards phone-embedded tracking. *Computers in Human Behavior*, *78*, 174–182. https://doi.org/10.1016/j.chb.2017.09.034

Lehtiniemi, T., & Kortesniemi, Y. (2017). Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach. *Big Data & Society*, *4*(2), 1–11. https://doi.org/10.1177/2053951717721935

Livingstone, S. (2006). Children's privacy online: Experimenting with boundaries within and beyond the family. In R. Kraut, M. Brynin, & S. Kiesler (Eds.), *Computers, phones, and the internet: Domesticating information technology* (pp. 145–167). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780195312805.003.0010

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, *10*(3), 393–411. https://doi.org/10.1177/1461444808089415

Lyon, D. (Ed). (2003). *Surveillance as social sorting: Privacy, risk and digital discrimination.* Routledge. https://doi.org/10.4324/9780203994887

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200–216. https://doi.org/10.1080/01972243.2016.1153012

Marwick, A. E., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Marwick, A., & Hargittai, E. (2018). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–157.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and integrity of social life.* Stanford University Press.

Oostveen, A., Vasalou, A., van den Besselaar, P. & Brown, I. (2014). Child location tracking in the US and the UK: Same technology, different social implications. *Surveillance & Society*, *12*(4), 581–593. https://doi.org/10.24908/ss.v12i4.4937

Prior, L. (2020). Content analysis. In P. Leavy (Ed.), *The Oxford handbook of qualitative research* (2nd ed.) (pp. 541–573). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780190847388.013.25

Regan, P. M., & Steeves, V. (2010). Kids R us: Online social networking and the potential for empowerment. *Surveillance & Society*, *8*(2), 151–165. https://doi.org/10.24908/ss.v8i2.3483

Rost, F. (2021). Q-sort methodology: Bridging the divide between qualitative and quantitative. An introduction to an innovative method for psychotherapy research. *Counselling and Psychotherapy Research*, *21*(1), 98–106. https://doi.org/10.1002/capr.12367

Sipior, J. C., Ward, B. T., & Volonino, L. (2014). Privacy concerns associated with smartphone use. *Journal of Internet Commerce*, *13*(3–4), 177–193. https://doi.org/10.1080/15332861.2014.947902

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1902.

Statistics Finland. (2021). *Väestön tieto- ja viestintätekniikan käyttö* [*The information and communication technology use of the population*]. https://www.stat.fi/til/sutivi/2021/sutivi_2021_2021-11-30_fi.pdf

Steeves, V., & Regan, P. (2014). Young people online and the social value of privacy. *Journal of Information Communication and Ethics in Society*, *12*(4), 298–313. https://doi.org/10.1108/JICES-01-2014-0004

Stoilova, M., Livingstone, S., & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, *8*(4), 197–207. https://doi.org/10.17645/mac.v8i4.3407

Sukk, M., & Siibak, A. (2021). "My mom just wants to know where I am": Estonian pre-teens perspectives on intimate surveillance by parents. *Journal of Children and Media*, *16*(3), 424–440. https://doi.org/10.1080/17482798.2021.2014646

Trochim, W. M. K. (1985). Pattern matching, validity, and conceptualization in program evaluation. *Evaluation Review*, *9*(5), 575–604. https://doi.org/10.1177/0193841X8500900503

Vickery, J. R. (2015). 'I don't have anything to hide, but... ': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294. https://doi.org/10.1080/1369118X.2014.989251

Westin, A. F. (1967). *Privacy and freedom.* Ig Publishing.

Widmer, S., & Albrechtslund, A. (2021). The ambiguities of surveillance as care and control: Struggles in the domestication of location-tracking applications by Danish parents. *Nordicom Review*, *42*(S4), 73–93. https://doi.org/10.2478/nor-2021-0042

Williams, S., & Williams, L. (2005). Space invaders: The negotiation of teenage boundaries through the mobile phone. *The Sociological Review*, *53*(2), 314–331. https://doi.org/10.1111/j.1467-954X.2005.00516.x

Wisniewski, P. J., Vitak, J., & Hartikainen, H. (2022). Privacy in adolescence. In B. P. Knijnenburg, X. Page, P. Wisniewski, H. Richter Lipford, N. Proferes, & J. Romano (Eds.), *Modern socio-technical perspectives on privacy* (pp. 315–336). Springer. https://doi.org/10.1007/978-3-030-82786-1_14

Yan, Z. (2018). Child and adolescent use of mobile phones: An unparalleled complex developmental phenomenon. *Child Development*, *89*(1) 5–16. https://doi.org/10.1111/cdev.12821

Endnotes

[1] The action or practice of sending sexually explicit photographs or messages via mobile phone.

[2] The list of stimulus items was originally created in the eQuality Project (see the acknowledgements). Items were listed based on a mainstream media search looking for any reports in newspapers, news magazines, and news sites that mentioned what a smartphone knows about its user.

CHAPTER 8

Omnipresent publicness

Social media natives and protective strategies of non-participation in online surveillance

LUISE SALTE

DEPARTMENT OF MEDIA AND SOCIAL SCIENCES, UNIVERSITY OF STAVANGER, NORWAY

ABSTRACT
People's perceptions of and experiences within online spaces are central to understanding implications of current online surveillance mechanisms. The aim of this study was to gain insight into how people accustomed to online spaces as part of social life negotiate social media as private and public spaces. This study drew on in-depth interviews with "social media natives" in Norway for this purpose. The interview data especially pinpointed two analytically separable, but currently empirically interchangeable, factors that were pivotal to the interviewees' negotiations of private and public space: the Internet's lack of temporal and spatial boundaries and social media's distributive logic. While the interviewees took these features of the online for granted, they explained feeling potentially surveilled by anyone, at any time, and thus acting accordingly. As social media that utilise people's data for economic profit are increasingly providing spaces for people's interactions, these feelings of uncertainty and surveillance prompts questions about the future role of prominent social media.

KEYWORDS: online participation, social media use, social media logic, public space, private space

Salte, L. (2023). Omnipresent publicness: Social media natives and protective strategies of non-participation in online surveillance. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 167–186). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-8

Introduction

In its early phases, the Internet prompted utopian visions of how it would revolutionise public sphere participation and citizens' agency (Coleman, 2005; Lindgren, 2017; Quandt, 2018). A society was envisioned where everyone would participate in public discussions and have their voice heard on equal terms. As social media platforms have become ever more important for information and communication practices (Flamingo, 2019; Newman et al., 2020), this would mean that digitalised societies experienced flourishing public spheres of citizens engaging in public discussion. However, while some point to the Internet as a place where people with not much debate experience can train for political participation (Winsvold, 2013), other studies indicate that people do not see online spaces as arenas fit for public conversation (Moe et al., 2019). Social media pose challenges to managing audiences and social contexts (Papacharissi, 2010; Velasquez & Rojas, 2017).

While social media platforms vary in terms of the combinations of strong and weak ties they afford (Goyanes et al., 2021), a distinct feature of the online world is that borders are lacking between what is public and private (Jensen, 2007). Facing a potential collapse of social contexts (boyd, 2014), people may engage in self-censorship practices (Velasquez & Rojas, 2017). Furthermore, a logic of virality and maximum exposure developed for corporations' economic profit currently steer how interactions travel on social media (Klinger & Svensson, 2015). Some argue that the ideals underlying and shaping social media platforms must be changed for the purpose of healthy societies (Brevini, 2013; Fuchs, 2014), while others advocate for more transparency regarding how social media companies use people's data (Demertzis et al., 2021). The relevance and urgency of such criticisms are echoed in research suggesting that people increasingly feel monitored online (Andersson et al., 2020; Fulton & Kibby, 2017). However, being attentive to surveillance mechanisms does not mean that one is necessarily concerned about corporate surveillance or how one's personal data is used. The concept of social privacy explains how some individuals may first and foremost see *other people* as potential violators of their privacy online, rather than the corporations that own social media (Demertzis et al., 2021; Park et al., 2018). While research on people's perceptions of algorithms is growing (Bucher, 2018; Fletcher & Nielsen, 2019; Hargiatti et al., 2020; Swart, 2021), more research is needed to grasp the complex, non-binary responses to social media as private and public spaces.

Social media are especially ingrained in young people's lives (boyd, 2014; Moe & Bjørgan, 2021). Usage purposes are wide, ranging from self-expression and entertainment to learning and engagement (e.g., Hautea et al., 2021). Notably, social media have become crucial to upholding and staying in touch with offline-anchored relationships (McRoberts et al., 2019; Thomas et al., 2017). Research shows that young people negotiate the perceived risks and benefits of social media use rather than merely resist or comply (Debatin et al., 2009). The concept of social media natives describes young adults who have grown up with social media (see, e.g., Brandtzæg, 2016). This study is guided by the following research question: How do social media natives negotiate social media as private and public spaces?

The aim of this study is to capture and understand how people accustomed to online spaces as part of social life evaluated and used social media as private and public spaces. As social media platforms become increasingly prominent to citizens' interpersonal communication and to their connections to the larger public, this was considered a pertinent question to gain further insight into the role of current prominent social media in Norwegian society. The study focuses on the perspectives of 11 young adults in Norway for this purpose.

In the following, the theoretical framework of the study is outlined. Here, I present two overarching mechanisms in the current online world that I argue may prompt feelings and experiences of surveillance. One is the intangibility of the Internet as space. Another is that people are accustomed to the rationales underlying social media, emphasising virality and maximum exposure. While these two mechanisms may be treated as distinguishable surveillance features, they are not empirically separable, as I demonstrate in the analysis, after the material and methods are introduced. The analysis section further illustrates a negotiation of risks and benefits of social media, in which a protective strategy of non-participation when in public space is crucial to circumvent surveillance mechanisms. Lastly, implications of these findings are discussed, where the relevance of people's perceptions of online spaces and online surveillance is emphasised. Particularly, I argue in this chapter that the economic incentives of social media are intensifying forces to the concept of the "omnopticon" (Jensen, 2007).

Surveillance and behaviour

Surveillance is a term with many connotations that varies in different contexts and regions (Fuchs & Trottier, 2015; Lyon, 2017). One approach concerns whether, and how, people perceive and imagine surveillance in their surroundings and life situation, and how this affects their behaviour, participation, or engagement in social and public life (e.g., Foucault, 1975/1994; Lyon, 2017). In digital society, surveillance is not just less personal and direct than previously (see, e.g., Mathiesen, 1997), it is also less visible while simultaneously more encompassing. As in Foucault's panopticon, major players (e.g., corporations, governments) monitor citizens, and power and responsibility are harder to locate. Furthermore, there is no end or pause for online activity, and ordinary people surveil other people (Lyon, 2017). In other words, the Internet facilitates a mutual mediated surveillance, where everybody can watch everybody, continuously (Jensen, 2007). Terms such as lateral surveillance have thus come to describe peer-to-peer observation

(Andrejevic, 2004). In this chapter, I suggest that two features are particularly relevant for understanding how online spaces may facilitate surveillance imaginaries in democratic and digital countries. One is connected to people's perceptions of a boundaryless Internet. The other is connected to people's close acquaintances with the political economy of social media.

First, the Internet and its boundaries between spaces cannot be seen by citizens interacting online. To that end, the Internet disrupts space. Furthermore, the online world has no time limits or curfew: It reaches different time zones and disrupts previous (more set) time frames for the public sphere and social spaces. Hence, the Internet lacks the previously more easily grasped boundaries, both in spatial and temporal terms (see, e.g., Lindgren, 2017; Wittel, 2000). One's audience is, in other words, uncertain (boyd, 2014). As pointed out by Papacharissi (2010: 142):

> [Online social spaces may] collapse front and backstage into a single space, by allowing privately intended information to be broadcast to multiple public audiences, and delivering publicly produced information to private and intimately known audiences. Moreover, the individual must assess not one situation, but potentially an infinite number, in which the same self-performance must maintain authenticity, coherence, and relevance.

Goffman (1959) theorised how people continuously engage in self-performance practices, moulding certain self-presentations as frontstage behaviours, which, unlike backstage behaviours, are oriented towards an audience and make use of "expressive equipment" to manage how one is seen (see, e.g., Goffman, 1959: 13). Papacharissi (2010), however, illustrated that managing how one is seen may be a rather complicated task online. Meyrowitz's (1985) theorisation of how electronic media disrupt previously set physical socialisation places for different stages of life becomes evident.

The boundaryless nature of the Internet makes what is public and personal blurred and ambivalent. While a blurring of the personal and the public is not a consequence of social media itself (Andersen, 2020), it may be especially relevant there (boyd, 2014). As found by Vatnøy (2017), people's online practices add elements to their profile, which in turn is taken to represent the totality of their identity and preferences. When lacking boundaries as defining mechanisms, new and constant evaluations are required. In highly digital societies such as the Nordics (Skogerbø & Karlsen, 2021), definitions of private and public are consequently not as easily set as they were in predigital times. Jensen's (2007) term omnopticon provides a useful account of these mechanisms' stimulation of an *ongoing* public sphere.

The concept of the public sphere originates from Habermas (1989) and describes public discourse arenas as inherent parts of a functioning democracy. According to deliberative theories, the public sphere must be free from financial and political interests to serve its proper function and to enable equal and free participation in discussions concerning shared concerns (Habermas, 1991). How people perceive the public sphere, its boundaries, and its barriers thus also matters to public participation. The omnopticon explains that the Internet has become a place of ceaseless mutual observation.[1] The social control mechanisms of Foucault's (1975/1994) panopticon and Mathiesen's (1997) synopticon[2] are combined, and the Internet's disruption of borders makes the public sphere never-ending, as observation of others is a characteristic of the public sphere (Jensen, 2007). Moreover, as borders or spaces cannot be used to define what is public online, "publicness must be defined solely in social terms, as mental processes, within and between individuals" (Jensen, 2007: 362). The term publicness reflects that when there is a lack of distinct and static places that can easily differentiate the public and the private, then spaces, interactions, and expressions can become defined or understood as part of public life. Thus, while a public space may be treated as a place – and hence a noun – public*ness* describes an adjective, inviting a description of the state or quality of *being*.

When suggesting the omnopticon, Jensen (2007) does not, however, consider one additional mechanism currently thriving upon the Internet's lack of borders that may further engender imaginaries of never-ceasing lateral surveillance. The second feature of online spaces that facilitates surveillance mechanisms is namely people's close acquaintances with the distributive logics of social media – a trait of the political economy of social media. This describes platforms' economically incentivised handling of people's data and interactions. While the way in which platforms infringe upon privacy – and collect and utilise people's data – is usually invisible (Debatin et al., 2009), the coding and datafication of people's movements and interactions has become normalised (van Dijck, 2014). The way communication and information commonly flow in online spaces is hence not entirely decided by users themselves. Instead, a logic of virality and maximum exposure impacts how communication travels within and across online spaces (Klinger & Svensson, 2015). Social media's logics – aiming for a maximum exposure of content and profiles – further engenders potential unknown audiences and surveillance agents in other users. When these circumstances are normalised as inherent to the online world, accompanied by blurry boundaries as explained above, unquestioned surveillance imaginaries and protective strategies may be instigated.

Material and methods

Eleven in-depth interviews with Norwegian young adults were conducted for the purpose of this study. Norway facilitates most of its citizens with the infrastructure required for taking part in "the digital" (European Commission, 2021), and as much as 82 per cent of the Norwegian population used social media on an average day in 2021 (Medienorge, 2022). As in the other Nordic countries, the Internet has become increasingly relevant to public communication in Norway (see, e.g., Skogerbø & Karlsen, 2021). The interviewees – six women and five men – can be described as social media natives (see, e.g., Brandtzæg, 2016). Born between 1992–2001, most (if not all) of their youth had been spent with social media and the smartphone ingrained in their social life. Their perceptions of social media as private and public spaces were thus particularly interesting, as they represent the most accustomed (adult) generation to our current media environment. As generational status often matters to one's perception and use of technology (Fang et al., 2019), a study of this particular group of individuals was considered interesting because they could give novel insights to, and potential prospects for, the role of increasingly relevant communication arenas.

The interviews were held between January 2020 and February 2021 (with a gap between April–December 2020 because of national Covid-19 restrictions). The interviews provided material for a more in-depth understanding of the use and perception of prominent digital social spaces; thus, the informants did not need to be representative of a population. The informants were all students at a Norwegian university, signing up for interviews via e-mail. They were all given non-gendered pseudonyms for anonymisation purposes. The interviews lasted from 1.5 to 2.5 hours and were semi-structured. The interviews started out with broad questions, talking about the informants' everyday lives and general media use. We then moved into more narrow areas and topics (see, e.g., Hermanowicz, 2002). Topics and areas of interest were at this stage guided by the information the interviewee had given thus far, in relation to the research question.

The later stages of each interview were guided by the photo elicitation technique (see, e.g., Harper, 2002; Vassenden & Andersson, 2010). Posts from Instagram and constructed illustrations of comment sections adhering to some of these posts were used at this stage. Some posts were drawn from typical Norwegian "influencers", illustrating typical lifestyle posts (Abidin, 2016), while others were drawn from public individuals frequently addressing public issues (Salte, 2022). This method was fruitful as it helped elucidate the intricacies of taken-for-granted practices and the informants' experiences and feelings: It allowed for reflections and details. This allowed a fuller grasp of their considerations of appropriateness and necessity on social media as communicative spaces. Questions were thus not directly concerned with privacy and online surveillance (cf. Samuelsson, Chapter 6; Mäkinen & Junila, Chapter 7). The interviews were conducted in Norwegian. Quotes used in this text were translated by the author before a simple test for accuracy was done by a colleague of the author translating the same quotes. The quotes were then adjusted by the author and the colleague in conjunction into the version they now appear in.

Thematic analysis was utilised as a qualitative analytical tool (Braun & Clarke, 2006). This approach is useful to detect main themes across qualitative data such as interviews, enabling in-depth analysis of certain parts of the data (Braun & Clarke, 2006). It is useful when 1) looking for a pattern of meaning reoccurring across the dataset that 2) captures something essential regarding the aim of the research (Braun & Clarke, 2006). This approach allows for detecting main themes across the interviews of particular importance to the research question. Themes found at the latent level were especially interesting for the purpose of this study (Braun & Clarke, 2006). Interviewees, for example, continuously returned to describing hesitations to being visible, connected to (taken-for-granted) online circumstances.

Analysis

Three key themes were detected: 1) a hesitation to be visible in open and unsafe spaces, 2) a construction of closed spaces, and 3) information gathering and learning while revealing as little meaning as possible. While these were analytically separable, they overlapped empirically. The interviewees, for example, described the necessity of closed spaces as following from the characteristics of open spaces. In the following, the themes are described throughout three sections, where this relationship between themes is demonstrated.

Closed versus open space

Observing rather than creating – and being careful of how one presents oneself to others if doing the latter – is nothing new when it comes to online practices (Croteau & Hoynes, 2019; Yang et al., 2017). The informants of this study similarly described being generally reluctant to leave visible traces for others to interpret online; rather, they preferred being careful and as invisible as possible. Being careful entailed not disclosing traces with much meaning for others to interpret, and different online behaviours rendered different amounts of meaning: Meaning-scarce actions such as "likes" were less critical, while meaning-dense actions such as posts or long comments were riskier. Such cautions, however, pertained predominantly to open online spaces. The informants' explained feeling uncertain about who could see their interactions, as there were no borders or boundaries. Self-constructed one-to-one or few-to-few spaces, on the other hand, where unintended audiences did not have access, were seen entirely differently. There, users could create boundaries by invitation-only access. Examples frequently mentioned were Snapchat, Facebook's Messenger, and the direct message function of Instagram. The close attention to how different spaces had different boundaries can be illustrated by Vikan, when speaking about their preference for Snapchat and their two separate Instagram accounts:

> I use snapchat a lot. What I like about it is that you can, immediately when you post things on the story, it's like, eh, purpose, you are purposive or what it's called… I mean, you know who you reach. […] But even if I don't post stuff on Instagram that much, I use it for sending stuff. And in that case, it is also this thing about taking it away from, like… the public and in, kind of away from… what everyone else sees […] But like I said, I did make this… eh blogish profile on there also. That [profile] doesn't have anything to do with me, kind of. Because there is nothing personal or private there, right. So there, it's more like… either something like old photographs I find interesting or… like, a clip from a movie or a TV show I think is cool, and stuff like that.
>
> My personal profile [on Instagram] is connected to that profile, but not the other way around. So, that profile doesn't exist, or there's no… link to me, except that a lot of the people that follow me is people I know. But in my private profile which is… private, you must ask to follow. And inside there is the link to that new profile.

Vikan here demonstrated an attentive evaluation to how different social media platforms, and different functions within them, enables constructing different boundaries. Without certain borders, what one posts is put in front of potentially everyone: The boundaries are ways to hide from unwanted observation instead of dealing with an otherwise uncertain audience. Vikan created different spaces for different areas in their social life, to keep some of their activities away from public spaces. While those allowed to enter the most private online life of Vikan may have seen other versions of them in the form of different Instagram profiles, it did not go the other way around: The more private, the more need for management of the audience. Vikan also illustrated that the interviewees' strategies were tailored to the affordances of the platforms. Snapchat, for example, facilitates strong ties, and its primary function entails preselecting who is able to watch one's content: It relies on active sending of messages, images, and videos to the specific receivers one wants to reach. Unlike Instagram or Facebook, for example, Snapchat does not provide spaces (i.e., a "feed" or a "profile") where others can observe one's interaction traces and content without one's knowledge. Snapchat may thus be considered as more manageable in terms of social context (boyd, 2014), and audience (Jensen, 2007). As result, it requires less self-censorship than social media such as Facebook (see Velasquez & Rojas, 2017). Interviewees still, however, created closed spaces *within* Snapchat, too. This way, visual and verbal messages could be easily sent for a specific audience, who in turn could comment on and discuss what had been sent – in a shared space. As informants elaborated on where and how they participated online, the notions of open and closed spaces became apparent. Delving into these responses disclosed imaginative surveillance mechanisms in play.

Spatial and temporal uncertainty – "eternal publicness" – in open space

When asked why they were reluctant to participate outside of spaces such as Snapchat and Facebook's Messenger, the informants described a lack of control, and uncertainty, in open spaces. As boundaries were fluid and intangible in open spaces, interactions were available to potentially anyone. Moreover, as interactions and utterances were somehow datafied, they could travel anywhere and be monitored at potentially any time in open spaces. Thus, uncertainties arose both in terms of time and space when interacting in open spaces, as they lacked temporal and spatial boundaries: Once data traces were left, they were left for eternity and were easily available to anyone on the Internet, potentially travelling across platforms and spaces. So far, these notions of open space reflect the first theme, that is, a hesitation to be visible in open and unsafe spaces. The notion of a somewhat potential eternal publicness for things posted outside of closed spaces can be illustrated by Ask:

> Maybe I don't feel like writing anything, perhaps, a little bit, because I don't want to have this, eh… like, imprint on… digital media, so it is… […] I don't know… I just feel like I have always thought about what the consequences of posting stuff like that may be. That it is not always a good thing, one can always search to find a whole lot about a person if everything is out there. […] I just don't want everything weird that I write – not that I write that much weird stuff – but, laying, laying out there for the public, for everyone to see.

"Everyone", "out there", and "always" pinpoint how these perceptions of lacking boundaries, and thus control, are connected to space and time. As informants elaborated on their preferred online practices, their attentiveness to spacial boundaries reflected concerns and continuous grappling with a collapse of the public and the private online. In closed spaces, as opposed to open spaces, boundaries were considered more tangible by (a control of) audience. This has thus so far reflected the second theme: a construction of closed spaces. Any action outside of self-constructed spaces was an action in uncertain, potentially eternal, publicness. When talking about expressing opinions online, this became particularly clear.

Participation forms revealing as little meaning as possible

The informants did occasionally post outside of private self-created spaces. When doing this, posts largely entailed non-controversial and non-deviant content; for example, if something extraordinarily fun, "cozy", or exciting happened in their lives, some mentioned that they could publish on their Instagram story or make a regular post. Stories disappear after 24 hours, and posts remain part of one's profile. As the former had a short life span, unlike the more permanent post, the threshold for publishing there was lower. Informants could also interact with other people's post or comments, most often because they knew and wanted to socially support the creator. Some also mentioned sharing posts from organisations like Amnesty International, frequently posting about human rights issues. In most cases, the content of these posts was regarded as uncontroversial, though one informant mentioned abortion as a case with some controversy in the Norwegian public as one exception. This was described as a crucial issue for the informant, allowing them to step out of their typically (more) careful online behaviour. Whether controversial or not, the informants this pertained to would in any case repost in these instances, rather than adding additional text to the post.

In general, content or actions not containing or rendering much meaning or opinion at all were preferred. Posting a comment in a comment section, for example, would require verbal and visual *self-chosen* text, leaving room for an unknown interpreter to make meaning of it – actions such as "hitting the like button", less so. Such a least-information-dense content- or activity-rationale became particularly clear when discussing Instagram posts addressing public issues, such as gender inequality, sexual assault, and economic profit versus social responsibility of influencers in the Norwegian public. The use of public figures' publications on Instagram, and (made-up examples of) their corresponding comment sections, especially shed light on the informants' evaluations of appropriate and inappropriate behaviours. The informants often spoke in a light persiflage, chuckling or shaking their head in these instances. Moreover, some told stories of their own experiences with others' strange or inappropriate behaviour online, for example, people writing certain comments in public comment sections or sharing things excessively. Their own behaviours, on the other hand, were taken as a given, naturally leading from the online environment. Informants preferred not to engage with the posts shown to them, or posts of similar publicness visible for others to see. When asked what they would do in the comment section of a post, if they had to, the informants chose participation forms conveying as little meaning as possible. They would typically "tag" a friend in the comment section, or simply post an emoji. My intention in asking this was not to get information on their actual online practices, but to dig further into their views and negotiations. For instance, Finley explained:

> I usually don't write anything, it's like... I would "tag" and then we would write in the chat instead.
>
> Me: Why?
>
> I think it's just... again, that I don't necessarily want to put my opinion out there. [...] I want to stay very neutral when it comes to my opinion... with the kind of stuff that might be a bit... so-so, when it comes to what other people think. And we rather just talk in the chat, with my friends.

As a feature commonly provided by social media, the tagging ("@-ing") enables communication between people, by notifying and showing to each other.[3] The action of tagging someone in a comment section can be seen as a kind of reciprocity. It is, however, performed in ways where outsiders cannot make sense of the meaning lying behind the tagging as long as no additional information is given in terms of emojis or text. The informants explained that they could find entertaining, informative, or interesting content outside of closed spaces, and by tagging someone in a corresponding comment section, further discuss it somewhere else, away from the eyes of others. Sending the content to a self-created space within the same social media platform provided the same functions. Risks were here mitigated; information would not suddenly end up in front of an unintended audience. That way, they could safely talk and keep in touch with friends and family, and also share and discuss news and common affairs. The last theme – information gathering and learning while revealing as little meaning as possible – shows in the activities that the interviewees described as appropriate and safe *enough*, in open spaces. They preferred content and actions that did not convey much meaning when interacting visibly in online open spaces, different from when interacting in offline settings or in private closed spaces online. As Kersten, a youth politician, said:

> Based on my Facebook profile, I don't think anyone would even think that I am politically active.

Discussion: Negotiations of online spaces in omnipresent publicness

While the social media natives used their smartphones and social media throughout their day, they all shared a taken-for-granted reluctance to participate in online spaces they regarded as open. The hesitation was reasoned in uncertainties of audiences and how and where their data travelled (e.g., Klinger & Svensson, 2015. Online, interactions prevailed and flowed in uncertain ways (Jensen & Helles, 2017): Beginnings and ends were unknown, and therefore, also audiences (boyd, 2014; Jensen, 2007). What could be carved out from these responses was notions of temporal and spatial uncertainties. Spatial uncertainties pertained to the fluid boundaries between spaces online (i.e., both within and across platforms) (e.g., Wittel, 2000). Temporal uncertainties pertained to time – interactions were potentially stored and available for others for eternity, seen from the social media natives' point of view. These uncertainties pertained to everything outside of spaces where boundaries were self-drawn by invitation-only access.

In closed spaces, on the other hand, the interviewees could discuss and share funny or interesting content and news. Closed spaces were thus valuable for upholding social relationships and for discussing and understanding public matters (Winsvold, 2013). A "special (socialisation) place" (Meyrowitz, 1985: 157) online was enabled, as they controlled entrance and thereby both current and potential future audiences. They were isolated together, separated from outsiders (Meyrowitz, 1985). It should be noted, however, that the interviewees described *imaginaries* of complete separations from outsiders. Social media discussions and content distributed in what is perceived as private spaces are not necessarily, or will not forever remain, private (Hasinoff, 2012). Imaginaries, however, shape practices (Lyon, 2017). To the interviewees, the notions of open and closed spaces were essential to their negotiations of private and public spaces, and hence online practices. If they participated visibly in spaces that were not closed-off, unclear agents could potentially watch from somewhere not predicted or foreseen. In these cases, they could not know if, how, or when they were being monitored. If wanting to be in control of how they were perceived by current or future others, they needed to act as if they were being constantly watched. In other words, they "adjust(ed) their behavior as though" potentially being "monitored constantly" online (Jensen, 2007: 371).

The mechanisms explained by Foucault's (1975/1994) panopticon metaphor become evident: The actual observation is not certain or needed. Internal notions of being watched are sufficient for the behavioural consequences to be in play. The interviewees' worries may reflect social privacy concerns (Demertzis et al., 2021; Park et al., 2018). Other people were, however, not seen as *violators* of privacy – as intentional surveillance agents that aimed to laterally surveil them (Andrejevic, 2004) – but were rather considered potential audiences to an online utterance or action due to how the Internet, in their words, just works, or is. Collapsed contexts and imaginaries of audiences are inherent features of the online world, and they affect how people behave online (boyd, 2014; see also Meyrowitz, 1985). Social media enables an environment where front- and backstage may collapse, forcing the individual to "assess not one situation, but potentially an infinite number, in which the same self-performance must maintain authenticity, coherence, and relevance" (Papacharissi, 2010: 142). Everything is potentially up for publicness (Jensen, 2007). This may put heavy demands on individuals who are concerned not only with current, but also future, impression management (Goffman, 1959). boyd (2014: 32) proposed that teens deal with these circumstances by imagining the audience they want to reach, as it is "impossible and unproductive to account for the full range of plausible interpretations".

The findings of this study indicate that when accustomed to a logic of virality, such a strategy may no longer be feasible. The likelihood of "going viral" and reaching unwanted attention may be too high. Having grown up with social media as part of their daily life, the young adults of this study had lifelong experience with the logics and structures of social media (Jensen & Helles, 2017), and the online as a boundary-scarce space (Wittel, 2000).

The intangibility of the Internet was seen as a natural part of the Internet (Jensen, 2007) – so too was a logic of virality (Klinger & Svensson, 2015). Facing these features of the online, the social media natives of this study rather *do* "go out of their way to make minutia private" (boyd, 2014: 62). They embrace a mentality of keeping privacy through effort, resisting the "widespread public-by-default" setting of the Internet (boyd, 2014: 62). To that end, they demonstrated a continuous struggle with collapsed contexts and audiences that they cannot see or determine, as part of their everyday life (boyd, 2014).

Their explanations display that two surveillance mechanisms are interlinked in synergic effect, which may intensify the need to be attentive in omnoptic circumstances. Their elaborations elucidate how feelings of being surveilled may be accentuated when one is accustomed to for-profit social medias' non-transparency and logic of distributing content. Like in Foucault's panopticon, they were aware of potentially being monitored by someone they couldn't see or predict, while being certain that surveillance was *somehow* present, and had an incentive. While the Internet's intangible nature opens the possibility of surveillance by unknown others at any time, social media's logic of virality promises its likelihood. The social media native's familiarity with social media's logic of virality and non-transparency may accentuate imaginations of ubiquitous surveillance, then. Consequently, they modify their behaviour as potentially monitored at any time in spaces they regard as open.

The social media natives' elaborations elucidate experiences of living in and with spaces of unceasing mutual surveillance (Andrejevic, 2004), and thus an omnopticon in play (Jensen, 2007). Mutual observation is a characteristic of the public sphere (Jensen, 2007), and it may thus become all-pervasive in spaces where boundaries cannot be seen or controlled. Omnipresent publicness describes such a boundaryless environment, where the public is everywhere and constantly encountered – it is a quality of the environment. It hence describes the omnoptic effect theorised by Jensen (2007). This study shows that such an environment may especially matter, and pose challenges, when a logic of virality reigns.

The informants' strategies must be further contemplated, however, as they may reflect specific social positions, media access, and literacy. If this study had been carried out elsewhere, the findings would likely be different. Education and income may, for example, conjunctly affect people's access and use of technologies (Fang et al., 2019). The interviewees were not just university students but had grown up in a country where a large majority of the population use the Internet and mobile platforms (Skogerbø & Karlsen, 2021). Furthermore, the interviewees largely presented as members of the majority, being white (Fang et al., 2019), presenting as cisgender and not differently abled, and speaking fluent Norwegian. This matters for understanding their responses, as research on online aggression and incivility, for example, indicates that minorities in Norway are most often the targets of such acts

(Sønsteby, 2020). Their situated privileges (Fang et al., 2019) in these regards likely shaped their experiences and expectations of the social media environment in ways that, for others, are not as available. Research considering the relation between socioeconomic factors and political participation has shown that a range of different factors can prompt non-participation (Laurison, 2015). The social media natives interviewed in this study explicitly pointed to one barrier relevant to their hesitation to participate visibly in open spaces: the uncertainties of the Internet as space, and the threat of virality.

Their high attentiveness to audience may reflect a need for impression management. Managing how they present before current and future audiences may be especially pertinent to them at the time the interviews were held, for example, being young adults and students, they may be particularly concerned with identity, career, and future (e.g., Mazalin & Moore, 2004). When they have no control over where and when their communication and interactions may appear, what is left for impression management and control of social context may be not leaving any communicative traces at all. When facing what is seen as unfavourable or risky online environments, inclination towards non-participation thus works as a strategy.

Social media holds prominent roles to the distribution of information and perspectives in the Norwegian public today (e.g., Moe & Bjørgan, 2021; Skogerbø & Karlsen, 2021). Previously, main distributors were more closely connected to, and could more easily be held accountable to, journalistic principles with democratic purposes (see Napoli & Caplan, 2017; Sjøvaag, 2010). While traditional public service media holds a strong presence in Norway, current prominent social media are largely steered by economic principles (Moe & Bjørgan, 2021). Surveillance mechanisms may partly be a function of people experiencing the online world as not embodied in matter, different from the more tactile offline world. As shown in this study, however, surveillance imaginaries are also connected to social media's logic of virality and rationale of maximum exposure, leading from social medias' profit incentives (Jensen & Helles, 2017; Klinger & Svensson, 2015) – that is, in addition to the purposive monitoring of users for economic profit (Fuchs, 2014).

Not only does social media work as a medium, transferring communication and information among citizens like traditional distributors, but it also provides and augments communicative spaces. If social media are relevant to interactions in the public sphere, the interviewees are, in other words, accustomed to profit rationales steering how communication and information travels in parts of the public sphere. Economic rationales steering parts of the public sphere invites using the public sphere as a critical concept to scrutinise "the shortcomings of societies" (Fuchs, 2014: 63). The public sphere should ideally be free from economic and political power to reach equal and free participation in discursive democracy (Habermas, 1991). Deliberative democracy both depends on and facilitates a low threshold for citizens' participation in conversations of common concern. Tearing down barriers is thus a part of the democratic project. If something makes people refrain from participating in such discussions, then it may be considered a barrier and a challenge to reach a healthy public.

Previous research has indicated that people do not see social media first and foremost as places for public debate (e.g., Moe et al., 2019). Likewise, the informants of this study mostly use social media for private sphere purposes (see Fuchs, 2014). To them, social media may first and foremost be spaces for upholding social relationships and for discussing and understanding public matters and disputes privately. To that end, social media natives' use of social media is valuable in a participatory democratic view insofar as it facilitates political participation training and preparation (e.g., Dahlgren, 2005; Pateman, 1970; van Dijck, 2000; Walker, 2005). Otherwise, it is a space of mutual never-ending surveillance by unknown audiences, both in terms of space and time. It is taken for granted that social media entails unknown present and future audiences, and that interactions are *somehow* stored and handled. The strategy of non-participation as default, as a response to surveillance imaginaries, thus poses further questions for the role of social media in digital societies such as the Nordics. As research continues to show the relevance of social media to public conversations, this is a particularly pertinent question: What kind of spaces are for-profit online social spaces becoming?

Scholars have long advocated for developing social media in line with public service ideals for the sake of democracy. Brevini (2013), for example, has argued that the Internet should "be infused with the same public service ethos [that] characterised traditional broadcasting" (2013: 157), through new policies focused on implementing public service ideals. Fuchs (2014) similarly advocated for an Internet in line with public sphere ideals as a response to neoliberalism's – up until then – legitimising effects of surveillance and profit-incentives in social media. Yet since these advocacies, the social media natives have for almost ten years lived with for-profit social media as part of their social life and public sphere (e.g., Andrew & Baker, 2021). Other scholars have, in more recent years, proposed remedies that do not demand a complete transformation of social media platforms' structures and rationales per se. Demertzis and colleagues (2021), for instance, called for increased transparency through "explainable AI", as a response to users' lack of agency and control. This included algorithms that disclosed their functions and why they made certain decisions (Demertzis et al., 2021). Transparency could, in addition to holding corporations accountable, increase a sense of control as to how and where people's interactions travel. This could mitigate the surveillance imaginaries described in this chapter.

The findings of this study do not go against the privacy paradox (see Norberg et al., 2007), nor do they demonstrate concern with personal data protection. Though the study does not capture the social media natives' thoughts, for example, on their location or health data being accessed or shared, what it does capture is social surveillance imaginaries brought about by social media infrastructures and the Internet as provider of private and public spaces. It demonstrates that perceptions of the online world are crucial for if, when, and how people utilise social media, and hence how they negotiate private and public spaces.

Conclusion

The purpose of this study was to gain insight into how people accustomed to online spaces as part of daily social life evaluated and used social media as private and public spaces. It has shown that while the interviewees continued using dominant social media platforms for social benefits, they implemented protective strategies to circumvent what they perceived as risks. Benefits lie, to the interviewees, in the upholding and creation of community and close relationships, and information gathering and learning. These benefits are particularly reached through creating private and closed spaces where others may only enter if invited. The social media natives did not, however, see spaces outside of such private self-created locations as fit for public sphere discussion – not only for political and public issue conversations, but also not for *any* actions from which much meaning or opinion may be interpreted. Grappling with online spaces' lack of boundaries in both time and space, where traces are left and potentially stored for eternity, their best strategy to keep control of current and future audiences was refraining from leaving traces of (much) meaning. While it is still "impossible and unproductive" to take into consideration all potential social contexts and audiences one may reach when posting on social media, the social media natives of this study responded to these circumstances by actively resisting the "widespread public-by-default" setting of the Internet (boyd, 2014: 32, 62). Their elaborations illuminate that the distributive logics of social media may especially necessitate carving out private spaces, and otherwise largely refraining from visibly participating.

While Jensen, writing 15 years ago, emphasised the boundaryless Internet as ground for surveillance mechanisms from the state and between ordinary citizens, there is currently an additional factor to consider. Inscribed in social media structures, a logic of virality and tracking technology facilitate an environment that may intensify the surveillance mechanisms that Jensen's omnopticon describes. When in conjunction, they may prompt surveillance imaginaries (Lyon, 2017), and attentive negotiations of private and public space. Although this study demonstrates protective strategies, it also emphasises that people's responses to surveillance mechanisms cannot be theorised as either accepting or resisting. A lack of control of social contexts, and a distributive logic aiming for maximum exposure and taking advantage of the boundaryless Internet, is rather – by the social media natives of this study – considered inevitable, if wanting to continue being online.

References

Abidin, C. (2016). Visibility labour: Engaging with influencers' fashion brand and #OOTD advertorial campaigns on Instagram. *Media International Australia*, *161*(1), 86–100. https://doi.org/10.1177/1329878X16665177

Andersen, I. V. (2020*). Instead of the deliberative debate: How the principle of expression plays out in the news-generated Facebook discussion* [Doctoral dissertation, University of Bergen]. http://hdl.handle.net/1956/24058

Andersson, J., Bäck, J., & Ernbrandt, T. (2020). *Svenskarna och internet 2020* [*The Swedes and the Internet 2020*]. The Swedish Internet Foundation. https://svenskarnaochinternet.se/app/uploads/2020/12/internetstiftelsen-svenskarna-och-internet-2020.pdf

Andrejevic, M. (2004). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479–497. https://doi.org/10.24908/ss.v2i4.3359

Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, *168*, *565–578*. https://doi.org/10.1007/s10551-019-04239-z

boyd, d. (2014). *It's complicated: The social lives of networked teens*. Yale University Press.

Brandtzæg P. B. (2016). The social media natives. In E. Elstad (Ed.), *Digital expectations and experiences in education* (pp. 149–162). SensePublishers. https://doi.org/10.1007/978-94-6300-648-4_9

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–102. https://doi.org/10.1191/1478088706qp063oa

Brevini, B. (2013). *Public service broadcasting online: A comparative European policy study of PSB 2.0*. Palgrave Macmillan. https://doi.org/10.1057/9781137295101

Bucher, T. (2018). *If...then: Algorithmic power and politics*. Oxford University Press. https://doi.org/10.18261/ISSN.0805-9535-2019-01-06

Coleman, S. (2005). Blogs and the new politics of listening. *The Political Quarterly, 76*(2), 273–280. https://doi.org/10.1111/j.1467-923X.2005.00679.x

Croteau, D., & Hoynes, W. (2019). *Media/society. Industries, images, and audiences* (6th ed.). Sage.

Dahlgren, P. (2005). The Internet, public spheres, and political communication: Dispersion and deliberation. *Political Communication*, *22*(2), 147–162. https://doi.org/10.1080/10584600590933160

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Demertzis, N., Mandenaki, K., & Tsekeris, C. (2021). Privacy attitudes and behaviors in the age of post-privacy: An empirical approach. *Journal of Digital Social Research*, *3*(1), 119–152. https://doi.org/10.33621/jdsr.v3i1.75

Doyle, A. (2011). Revisiting the synopticon: Reconsidering Mathiesen's 'The Viewer Society' in the age of Web 2.0. *Theoretical Criminology*, *15*(3), 283–299. https://doi.org/10.1177/1362480610396645

European Commission. (2021). *The digital economy and society index (DESI)*. https://digital-strategy.ec.europa.eu/en/policies/desi

Fang, M. L., Canham, S. L., Battersby, L., Sixsmith, J., Wada, M., & Sixsmith, A. (2019). Exploring privilege in the digital divide: Implications for theory, policy, and practice. *The Gerontologist*, *59*(1), e1–e15. https://doi.org/10.1093/geront/gny037

Flamingo. (2019). *How young people consume news and the implications for mainstream media*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-02/FlamingoxREUTERS-Report-Full-KG-V28.pdf

Fletcher, R., & Nielsen, R. K. (2019). Generalised scepticism: How people navigate news on social media. *Information, Communication & Society*, *22*(12), 1751–1769. https://doi.org/10.1080/1369118X.2018.1450887

Foucault, M. (1994). *Overvåkning og straff* [*Discipline and punish*]. Gyldendal Norsk Forlag. (Original work published 1975)

Fuchs, C. (2014). Social media and the public sphere. *tripleC: Communication, Capitalism & Critique*, *12*(1), 57–101. https://doi.org/10.31269/triplec.v12i1.552

Fuchs, C., & Trottier, D. (2015). Towards a theoretical model of social media surveillance in contemporary society. *Communications*, *40*(1), 113–135. https://doi.org/10.1515/commun-2014-0029

Fulton, J. M., & Kibby, M. D. (2017). Millennials and the normalization of surveillance on Facebook. *Journal of Media & Cultural Studies*, *31*(2), 189–199. https://doi.org/10.1080/10304312.2016.1265094

Goffman, E. (1959). *The presentation of self in everyday life*. Doubleday.

Goyanes, M., Borah, P., & Gil de Zúñiga, H. (2021). Social media filtering and democracy: Effects of social media news use and uncivil political discussions on social media Unfriending. *Computers in Human Behavior*, *120*, 106759. https://doi.org/10.1016/j.chb.2021.106759

Habermas, J. (1989). *The structural transformation of the public sphere*. Polity.

Habermas, J. (1991). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society* (T. Burger, Trans.). MIT Press.

Hargiatti, E., Gruber, J., Djukaric, T., Fuchs, J., & Brombach, L. (2020). Black box measures? How to study people's algorithm skills. *Information, Communication & Society*, *23*(5), 764–775. https://doi.org/10.1080/1369118X.2020.1713846

Harper, D. (2002). Talking about pictures: A case for photo elicitation. *Visual Studies*, *17*(1), 13–26. https://doi.org/10.1080/1472586022013734 5

Hasinoff, A. A. (2012). Sexting as media production: Rethinking social media and sexuality. *New Media & Society*, *15*(4), 449–465. https://doi.org/10.1177/1461444812459171

Hautea, S., Parks, P., Takahashi, B., & Zeng, J. (2021). Showing they care (or don't): Affective publics and ambivalent climate activism on TikTok. *Social Media + Society*, 1–14. https://doi.org/10.1177/20563051211012344

Hermanovicz, J. C. (2002). The great interview: 25 strategies for studying people in bed. *Qualitative Sociology*, *25*(4), 479–499. https://doi.org/10.1023/A:1021062932081

Jensen, J. L. (2007). The Internet omnopticon - surveillance or counter-insurgency? In H. Bang, & A. Esmark (Eds.), N*ew publics with/out democracy*. (pp. 351–380). Samfundslitteratur Press.

Jensen, K. B., & Helles, R. (2017). Speaking into the system: Social media and many-to-one communication. *European Journal of Communication*, *32*(1), 16–25. https://doi.org/10.1177/0267323116682805

Klinger, U., & Svensson, J. (2015). The emergence of network media logic in political communication: A theoretical approach. *New media & society*, *17*(8), 1241–1257. https://doi.org/10.1177/1461444814522952

Laurison, D. (2015). The willingness to state an opinion: Inequality, don't know responses, and political participation. *Sociological Forum*, *30*(4), 925–948. https://doi.org/10.1111/socf.12202

Lindgren, S. (2017). *Digital media and society*. Sage.

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication*, *11*, 824–842. https://ijoc.org/index.php/ijoc/article/view/5527/1933

Mathiesen, T. (1987). The eagle and the sun: On panoptic systems and mass media in modern society. In J. Lowman, R. J. Menzies, & T. S. Palys (Eds.), *Transcarceration: Essays in the sociology of social control* (pp. 59–75). Cambridge Studies in Criminology 55. Gower.

Mathiesen, T. (1997). The viewer society. Michel Foucault's 'Panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/10.1177/1362480697001002003

Mazalin, D., & Moore, S. (2004). Internet use, identity development and social anxiety among young adults. *Behaviour Change*, *21*(2), 90–102. https://doi.org/10.1375/bech.21.2.90.55425

Medienorge. (2022). *Bruk av sosiale medier en gjennomsnittsdag* [*Use of social media on an average day*]. Medianorway. https://www.medienorge.uib.no/statistikk/medium/ikt/412

McRoberts, S., Yuan, Y., Watson, K., & Yarosh, S. (2019, June). Behind the scenes: Design, collaboration, and video creation with youth. *Proceedings of the 18th ACM International Conference on Interaction Design and Children*, 173–184. https://doi.org/10.1145/3311927.3323134

Meyrowitz, J. (1985). *No sense of place: The impact of electronic media on social behavior*. Oxford University Press.

Moe, H., & Bjørgan, J. (2021). *Nordmenns bruk av digitale nyheter: Nyhetsbruk* [*Norwegians' use of digital news: Use of news*]. Reuters Digital News Report. https://nyhetsbruk.w.uib.no/

Moe, H., Hovden, J. F., Ytre-Arne, B., Figenschou, T., Nærland, T. U., Sakariassen, H., & Thorbjørnsrud, K. (2019). Sosiale medier [Social media]. In H. Moe, J. F. Hovden, B. Ytre-Arne, T. Figenschou, T. U. Nærland, H. Sakariassen, & K. Thorbjørnsrud (Eds.), *Informerte borgere? Offentlig tilknytning, mediebruk og demokrati* [*Informed citizens? Public connection, media use and democracy*] (pp. 72–91). Scandinavian University Press.

Napoli, P., & Caplan, R. (2017). Why media companies insist they're not media companies, why they're wrong, and why it matters. *First Monday*, *22*(5). https://doi.org/10.5210/fm.v22i5.7051

Newman, N., Fletcher, R., Schulz, A., Andi, S., & Kleis Nielsen, R. (2020). *Reuters Institute digital news report 2020*. Reuters Institute for the Study of Journalism, University of Oxford. https://www.digitalnewsreport.org/survey/2020/

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Papacharissi, Z. (2010). *A private sphere: Democracy in a digital age*. Polity.

Park, Y. J., Chung, J. E., & Shin, D. H. (2018). The structuration of digital ecosystem, privacy, and big data intelligence. *American Behavioral Scientist*, *62*(10), 1319–1337. https://doi.org/10.1177/0002764218787863

Pateman, C. (1970). *Participation and democracy theory*. Cambridge University Press. https://doi.org/10.1017/CBO9780511720444

Quandt, T. (2018). Dark participation. *Media and Communication*, *6*(4), 36–48. https://doi.org/10.17645/mac.v6i4.1519

Salte, L. (2022). Visual, popular, and political: The non-profit influencer and the public sphere. *Javnost – The Public*, *29*(4), 1–17. https://doi.org/10.1080/13183222.2022.2147776

Sjøvaag, H. (2010). The reciprocity of journalism's social contract: The political-philosophical foundations of journalistic ideology. *Journalism Studies*, *11*(6), 874–888. https://doi.org/10.1080/14616701003644044

Skogerbø, E., & Karlsen, R. (2021). Media and politics in Norway. In E. Skogerbø, Ø. Ihlen, N. N. Kristensen, & L. Nord (Eds.), *Power, communication, and politics in the Nordic countries* (pp. 91–111). Gothenburg: Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855299-5

Swart, J. (2021). Experiencing algorithms: How young people understand, feel about, and engage with algorithmic news selection on social media. *Social Media + Society*, *7*(2), 1–11. https://doi.org//10.1177/20563051211008828

Sønsteby, H. B. (2020). *Hate speech against religious queer women* [Master's thesis, University of Agder]. https://hdl.handle.net/11250/2685320

Thomas, L., Briggs, P., Hart, A., & Kerrigan, F. (2017). Understanding social media and identity work in young people transitioning to university. *Computers in Human Behavior*, *76*, 541–553. https://doi.org/10.1016/j.chb.2017.08.021

van Dijck, J. (2000). Models of democracy and concepts of communication. In K. L. Hacker, & J. Van Dijck (Eds.), *Digital democracy: Issues of theory and practice* (pp. 30–53). Sage. https://doi.org/10.4135/9781446218891.n3

van Dijck, J. (2014). Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Vassenden, A., & Andersson, M. (2010). When an image becomes sacred: Photo-elicitation with images of holy books. *Visual Studies*, *25*(2), 149–161. https://doi.org/10.1080/1472586X.2010.502672

Vatnøy, E. (2017). *The rhetoric of networked publics: Studying social network sites as rhetorical arenas for political talk* [Doctoral dissertation. University of Bergen]. http://hdl.handle.net/1956/17262

Velasquez, A., & Rojas, H. (2017). Political expression on social media: The role of communication competence and expected outcomes. *Social Media + Society*, 1–13. https://doi.org/10.1177/2056305117696521

Walker, T. (2005). Whose civics, whose citizen: Reconceptualizing U.S. democracy in the postindustrial era. In C. White, & R. Openshaw (Eds.), *Democracy at the crossroads* (291–310). Lexington Books.

Winsvold, M. (2013). Deliberation, competition, or practice? The online debate as an arena for political participation. *Nordicom Review*, *34*(1), 3–15. https://doi.org/10.2478/nor-2013-0039

Wittel, A. (2000). Ethnography on the move. *Forum Qualitative Sozialforschung*, *1*(1). https://doi.org/10.17169/fqs-1.1.1131

Yang, S., Quan-Haase, A., Nevin, A. D., & Chen, Y. (2017). the role of online reputation management, trolling, and personality traits in the crafting of the virtual self on social media. In L. Sloan, & A. Queen-Haase (Eds.), *The Sage handbook of social media research methods* (pp. 74–89). Sage. https://doi.org/10.4135/9781473983847

Endnotes

[1] Lyon (2017) presents similar accounts through the term surveillance culture, describing how multifaceted and ubiquitous surveillance is enabled by recent technological developments.

[2] While Mathiesen's concept of synopticon (1987, 1997) overlooks resistance (by only focusing on Foucault's panopticon, Mathiesen did, for example, not give much attention to Foucault's later emphasis on resistance when himself theorising the synopticon; see, e.g., Doyle, 2011), and indeed the Internet, it draws attention to the role of the media and surveillance mechanisms as theorised by Foucault. According to Mathiesen, the mass media had come to represent another system of social control, in parallel with the panopticon. A few people (such as journalists and celebrities) decided what a large (and passive) audience was exposed to.

[3] For example, when using the "@"-symbol followed by a person's username as part of a comment in a comment section, the person "owning" that username receives a notification that enables them to go directly into the comment section to the place where that comment is located. It thus enables responses, creating or continuing conversations by notifying others. To that end, it differs from sending the post (of which the comment section is attached) to people in a more private and closed space (such as in their "dm", short for direct message, on Instagram), and from "sharing" it (consequently making it a part of the content featured in the space connected to one's own personal profile).

CHAPTER 9

Kant's ethics in the age of online surveillance

An appeal to autonomy

CASEY RENTMEESTER
BELLIN COLLEGE, USA

ABSTRACT

Using Michel Foucault's conception of pervasive power, the purpose of this chapter is to analyse the contemporary paradigm of online surveillance from a philosophical perspective by unpacking the power dynamics involved in online surveillance, ultimately arguing, with McKenzie Wark, that there is an asymmetry of power that puts individual persons at risk. I then turn to Martin Heidegger's notion of *Gelassenheit* as a helpful way to think through what an intentional stance towards online surveillance might look like that does not escape the paradigm but is at least conscious of its influence. Finally, I utilise Immanuel Kant's ethics and political philosophy to provide recommendations as to the appropriate ethical relationships that should exist between individual persons, governments, and corporations, ultimately arguing that respect for personal autonomy – that is, the right to choose our lives in accordance with our interests – must be at the forefront of conversations regarding the ethics of online surveillance.

KEYWORDS: data ethics, Michel Foucault, philosophy of technology, Martin Heidegger, asymmetry of information

Rentmeester, C. (2023). Kant's ethics in the age of online surveillance: An appeal to autonomy. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 187–204). Nordicom, University of Gothenburg.
https://doi.org/10.48335/9789188855732-9

Introduction

A common metaphor regarding surveillance is "Big Brother" from George Orwell's classic work, *1984*, a dystopian novel in which citizens are constantly not only being watched but also reminded of such surveillance through the ubiquitously hammered slogan, "Big Brother is watching you" (Orwell, 1950). In his 2018 book, *The Culture of Surveillance*, David Lyon asks us to move beyond such Orwellian rhetoric when examining our contemporary age of surveillance, speaking of the ways in which we willingly submit to surveillance, thinking – perhaps – that we have nothing to hide. For Lyon (2018: 4), "watching has become a way of life" to such an extent that we live in what he calls "a culture of surveillance". Each click, tap, and scroll on our smart devices is tracked and stored in vast databases, which are then sent to algorithms tied to powerful artificial intelligence technologies that have the potential to manipulate future human behaviour. Under such a setup, one can genuinely be confused as to whether, for instance, the consideration of purchasing a product generated by an algorithm in a nudged advertisement from a recommendation engine is truly a reflection of one's interests or, in fact, a matter of manipulation.

I begin this chapter by arguing that Michel Foucault's conception of power might provide a helpful lens to understand the contemporary paradigm of online surveillance. Rather than the top-down sort of power that subjects experienced in the past from rulers, power must now be understood as "pervading the very fabric of society itself" (Foucault, 1984c: 61). Francis Bacon's (1899) age-old dictum that knowledge is power has been heeded by corporations in understanding that information is knowledge, which thereby provides power, thus explaining their redoubled efforts toward data analytics. Upon conceptually grounding the power dynamics at work in online surveillance through tactics like data collection and analytics, I turn to McKenzie Wark's (2019) latest work, *Capitalism is Dead*, where she provided insight into the power of information in the contemporary age, ultimately arguing that those who own and control information – Amazon and Google being obvious players, but also any institution that is putting the power of data analytics to work, including the university you may work for – are demonstrating that information may in fact be more powerful than capital itself. I then juxtapose Wark's thesis with the work of Shoshana Zuboff (2019), who argued that we live in the age of surveillance capitalism, which undermines personal autonomy and threatens democracy itself. Whether we frame surveillance from the perspective of Big Tech or in terms of the seemingly "self-chosen" surveillance by individuals, one cannot deny that surveillance is pervasive. How, then, are we to respond in our everyday lives if we are not entirely willing to submit? We cannot, as Martin Heidegger (1969: 40) noted, "reject today's technological world as devil's work, nor may we destroy it". I demonstrate that no matter how staunchly we oppose it by clinging to "dumbphones" over smartphones, typewriters over computers, or cash over debit cards, most contemporary persons in industrialised settings still have to reckon with the ubiquity of surveillance and "dance with the devil", as digital personal data is gathered through many of the basic institutions in modern society, including, for instance, the government, the electric company, or healthcare institutions. Using Heidegger's philosophy as a theoretical background, and particularly his notion of *Gelassenheit*, I try to show how we can use technological devices without allowing them to manipulate us, which is the first step in approaching an intentional stance towards online surveillance.

I end the chapter by utilising Immanuel Kant's conception of autonomy to provide an ethical lens with which to approach the age of surveillance. For Kant (2002: 51), "rational beings all stand under the law that every one of them ought to treat itself and all others never merely as [a] means, but always at the same time as [an] end in itself". If we take Kant seriously, we ought to respect the human ability to choose our lives in accordance with our interests and not subsume others' interests to our own without their consent. Moreover, if we treat our digital footprint – that is, the trail of clicks, taps, and scrolls – as an extension of ourselves in the vein of Marshall McLuhan (1964), then we should have a say as to who has access to that information, if we are to respect human autonomy. I conclude by examining some of Kant's thoughts on the role government plays in ensuring respect for human autonomy and apply it to the age of surveillance, arguing that the government has an obligation to limit the manipulation of consumers through the practice of data analytics by corporations but also that individual rights to autonomy for citizens must be protected from the government itself.

Pervasive power

The most influential philosophy of power espoused in the twentieth century certainly comes from Michel Foucault, who was deeply influenced by Friedrich Nietzsche (Rosenberg & Westfall, 2018). *The Will to Power*, a collection of Nietzsche's notes spanning from 1883 to 1888, famously ends with the unequivocal claim that "*This world is the will to power – and nothing besides!* And you yourselves are also this will to power – and nothing besides! [emphasis original]" (Nietzsche, 1967: §1067). While Foucault did not agree with all of Nietzsche's philosophical pronouncements, he seems to have taken Nietzsche's notion of the pervasiveness of power seriously. In commenting on its historical dynamics, Foucault juxtaposes the old versions of power that dominated premodern societies with contemporary versions of power. Whereas premodern power was exercised by rulers upon subjects, new methods of power are,

> not ensured by right but by technique, not by law but by normalization, not by punishment but by control [and entail] methods that are employed

> *on all levels* and *in forms that go beyond the state and its apparatus* [emphasis added]. (Foucault, 1990: 89)

Foucault (1995: 208) warns us of power being "exercised continuously in the very foundations of society, in the subtlest possible way". From a Foucauldian perspective, one cannot *escape* power, but one can become *more conscious* of its mechanisms and how it can affect our "acts, attitudes, and modes of everyday behavior" (Foucault, 1984c: 67). Foucault defines this activity of becoming more conscious as thought:

> [Thought] is what allows one to step back from this way of acting or reacting, to present it to oneself as an object of thought and question it as to its meaning, its conditions, and its goals. Thought is freedom in relation to what one does. (Foucault, 1984a: 388)

Engaging in thought entails taking a reflective stance and thinking through how we are affected by that with which we engage with on an everyday basis.

Foucault, of course, was not talking about online surveillance in these passages: He died of complications of HIV/AIDS in 1984 before the digital age in which the culture of surveillance – to borrow Lyon's (2018) phrase noted above – had become so pervasive (the World Wide Web was not publicly available until the early 1990s). Nevertheless, Foucault's philosophy of power provides a fitting conceptual lens from which to understand online surveillance. Indeed, Jan Peter Bergen and Peter-Paul Verbeek (2021: 326) have argued that the appropriation of Foucault's work on the ways in which technology has a formative influence on "the way we live, speak, think, and behave" is fitting. From a Foucauldian perspective, online surveillance must be understood as 1) embedded in various techniques; 2) pervasively normalised; and 3) a form of control. Techniques of online surveillance are polymorphous in nature. Examples of such techniques are as follows: surveillance cameras are now linked with the Internet and monitored constantly; any given action on one's smartphone can be tracked and analysed, including the exact location of one's device via the Global Positioning System (GPS); and various smart devices, from smartwatches to smart speakers, are continuously receiving and recording data. Surveillance has become so ubiquitous that we can regard it as "the new normal". Take, for instance, the normalisation of smartphones noted by Lyon (2018: 85–86):

> The smartphone is the embedded medium par excellence that connects users with data in everyday life. They are not just familiar, they are in many ways indispensable to contemporary life. They are used for many commercial transactions, including ticketing and online banking, as a way of being informed about breaking news, working out the ideal route for a trip, and checking what bodily symptoms might mean for personal health, among multiple other tasks.

Even those of us who have resisted adopting smartphones cannot escape the pervasiveness of online surveillance in other spheres, such as healthcare systems, governments, corporations, and utility providers that collect, coordinate, and analyse personal data regularly. McKenzie Wark (2019: 3) puts the point the following way: "These days, not just everyone but everything is tracked and monitored and turned into information". Thus, the first two aspects of online surveillance – its polymorphous nature and its pervasive normalisation – are straightforward. Given its pervasiveness, we cannot completely escape online surveillance in its various forms.

This leads us to the third Foucauldian aspect of online surveillance, the aspect of control, which calls for the most amount of philosophical reflection. Wark (2019: 26) has brilliantly outlined online surveillance as a form of control in her book *Capitalism is Dead*, where she offers the provocative thesis that poses "the possibility that capitalism has already been rendered historical but that the period that replaces it is worse". The worse era – *our* era – is the age in which information is "a *dominant* force of production [emphasis original]" (Wark, 2019: 46) that is exploited by "the new kind of ruling class":

> This new kind of ruling class does not appropriate a quantity of surplus value so much as exploit an asymmetry of information. It gives, sometimes even as a gift, access to the location of a piece of information for which you are searching. Or it lets you assemble your own social network. Or it lets you perform a particular financial transaction. Or it gives you coordinates on the planet and what can be found at that location. Or it will even tell you some things about your own DNA. Or it will provide a logistical infrastructure for your small business. But while you get that little piece of information, this ruling class gets all of that information in the aggregate. It exploits the asymmetry between the little you know and the aggregate it knows – an aggregate it collects based on information you were obliged to "volunteer." (Wark, 2019: 54–55)

The asymmetry of information leads to an imbalance in terms of control: Those who have the information have the power to control those who do not have it.

While we may not want to agree with Wark that we live in a post-capitalist age, we certainly should recognise the truth in the notion that there is great power in information – a truth echoed in the oft-quoted statement from Francis Bacon (1899) that knowledge is power. Those of us who still think capitalism is alive and well might find Shoshana Zuboff's concept of surveillance capitalism to be a more fitting description of our contemporary era. According to Zuboff (2019: 8), "surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data". She goes on to argue that "surveillance capitalism births a new species of power" called instrumentarianism that "knows and shapes human behavior toward others' ends" (Zuboff, 2019: 9), which is a threat to both human autonomy and democracy itself. Instrumentarianism can be defined as a form of power in which all entities – including human beings – are turned into mere means to ends, that is, instruments, to values or priorities above and beyond them. In the end, we are faced with what Zuboff (2019: 11) calls "a twenty-first-century Faustian compact", in which we are forced to give up fundamental rights to privacy to access even basic resources, given the normalisation of online surveillance. While Faust struck a deal with the devil and exchanged his soul for unlimited knowledge and worldly pleasures, our "dance with the devil" entails figuring out just how much information about ourselves we are willing to share (when, that is, we are given the option) with those in power in exchange for access to convenient technological devices that make everyday life easier to navigate.

Dancing with the devil

Whether we agree with Wark or Zuboff in terms of the status of capitalism in our contemporary era, it is clear there is pervasive power in online surveillance. The question is how we can respond as individuals to retain some sense of human autonomy. The first step, at least in my estimation, begins with Herbert Marcuse's (1964: 7) sense that "all liberation depends on the consciousness of servitude". We must begin to recognise what we are submitting to when we click "accept cookies", allow websites to access our location, agree to the terms and conditions of our various arrangements, or install smart devices into our homes or wear them on our bodies, to mention but a few examples of techniques linked to online surveillance. There are, however, situations in which we are not even offered the chance to provide our informed consent, which explains Zuboff's notion that we all must engage in some type of Faustian compact. For example, if we want to exercise our right to vote in a democracy, that automatically entails sharing information with the government; similarly, if we want access to electricity, that necessitates disclosing information to the electric company. Barring taking up an existence in which one is willing to live entirely "off the grid", everyone must, to some extent, submit to the current paradigm.

In this section, I use Heidegger's philosophy to think through how to navigate the ubiquity of online surveillance. For Heidegger (1969: 40), "we cannot, of course, reject today's technological world as devil's work, nor may we destroy it". We live in an inevitable technological age that includes some level of surveillance. Heidegger (1966: 52) argues that "it is not that the world is becoming entirely technical which is really uncanny. Far more uncanny is our being unprepared for this transformation, our inability to confront meditatively what is really dawning in this age". Having been born in the small town of Messkirch in Germany's Black Forest in 1889 and spending much of his life there, Heidegger thought deeply about the ways in which the age of modern technology was changing the human relationship with things, since he witnessed first-hand how technological advances led to the shrinking of "all distances in time and space" (Heidegger, 1971: 165). Thus, even though Heidegger did not witness the rise of the digital era, his thought has been utilised as a helpful theoretical lens to understand the ways in which the Internet changes our relationship to the world (Carabantes, 2021).

From a Heideggerian perspective, the question is not whether to submit to any and all surveillance for most humans living in the contemporary era, but rather, "what are some ways in which we can resist surveillance and maintain elements of autonomy?" Heidegger (1977: 4) argued that "everywhere we remain unfree and chained to technology, whether we passionately affirm or deny it" and warned of the dangers involved when "the laboring animal is left to the giddy whirl of its products so that it may tear itself to pieces and annihilate itself in empty nothingness" (Heidegger, 1973: 87). Heidegger was worried that the seemingly insatiable drives that persons demonstrate in the age of modern technology for satisfying material pleasures instantaneously – exemplified so clearly, for instance, in Amazon's same-day shipping or on-demand streaming services – is a sign of nihilism. His philosophy can help get us to step back and reflect on whether a life dedicated to efficiency, productivity, ephemeral entertainment, and material possessions is really a life worth living.

Having spent much of his career elucidating the complexities of Heidegger's philosophy, the contemporary American philosopher Richard Polt has tried to demonstrate alternative approaches to life wherein one does not completely disavow technology but is instead thoughtful about how one integrates technological devices into one's everyday life. Polt (2018: 75) argued that "the most desirable kinds of technology may be those that leave room for the non-technological – techniques and devices of limited scope that do not presume to intrude on every aspect of our lives". In *The Typewriter Revolution*, for instance, Polt outlined how individuals can resist the over-digitisation of our lives by writing with a typewriter rather than a computer. The work begins with the following manifesto:

> We assert our right to resist the Paradigm, to rebel against the Information Regime, to escape the Data Stream. We strike a blow for self-reliance, privacy, and coherence against dependency, surveillance, and disintegration […]. We choose the real over representation, the physical over the digital, the durable over the unsustainable, the self-sufficient over the efficient. (Polt, 2015: 6)

Polt (2015: 352) viewed the utilisation of typewriters as a revolt against "what the world has already become: a digital domain under automated surveillance". Other ways to resist online surveillance explicitly – to some extent or another –include choosing to listen to music on vinyl record players rather than smart speakers, reading a physical book rather than an e-book, using a mobile phone that is not a smartphone, or taking Polaroid pictures rather than digital ones. Such intentional stances explicitly repudiate the power of data analytics by detaching the experience from the ubiquitously surveilled online realm. Most of us cannot always choose these options. For instance, as a professor, I'm necessarily connected to the Internet by checking and responding to student e-mails, working in my university's learning management system, and so on. However, in certain aspects of our lives, we do have some choice: My choice to have a non-smartphone and listen to vinyl records in my personal life are examples.

Notice that none of these options entail a complete dismissal of technology but rather an intentional stance toward technology. Heidegger (1966: 54) discusses such a stance as follows:

> We can use technical devices, and yet with proper use also keep ourselves so free of them, that we may let go of them any time. We can use technical devices as they ought to be used, and also let them alone as something which does not affect our inner and real core. We can affirm the unavoidable use of technical devices, and also deny them the right to dominate us, and so to warp, confuse, and lay waste our nature.

Heidegger calls this comportment towards things *Gelassenheit* [letting be], which entails the same sort of approach that Foucault mentioned in his definition of thought noted above, that is, a "freedom in relation to what one does" (Foucault, 1984a: 388). Indeed, Heidegger (2010: 149) sees *Gelassenheit* and freedom as inherently linked and states, "as soon as we are capable of […] letting something be in that into which – as into its own essence – it is let, then we are truly free". At one point, Heidegger (1998b) actually defines freedom *as Gelassenheit*. When applied to technology and online surveillance, *Gelassenheit* entails a freedom *from* being manipulated and freedom *to* enact one's own possibilities that have been chosen by oneself. When I pull out an old vinyl record to play, for example, I can listen to the music I want to hear without worrying about my preferences being stored in a database so that a recommendation engine can suggest a new song in the future (Rentmeester, 2022b). Thus, an element of freedom is retained without having to worry about that experience being filed away and used in the future to manipulate my behaviour.

In his magnum opus, *Being and Time*, Heidegger (1962: 312) emphasises the importance of choosing one's own life and not getting "carried along" by others. His term *Eigentlichkeit* [authenticity] refers to taking ownership of our lives and not allowing ourselves to blindly submit to the interests of others. As Thomas Sheehan (2015: 262n49) notes, *Gelassenheit* "is the later parallel of the earlier 'authenticity'" [*Eigentlichkeit*]. Thus, to some extent, Heidegger shows an interest in what philosophers call autonomy, which is typically understood as the right to choose one's life in accordance with one's interests. Importantly, enacting Heidegger's notion of *Eigentlichkeit* does not entail a rejection of social norms that have pervaded society through normalisation (Burgess & Rentmeester, 2015). When applied to online surveillance, it is not a matter of trying to completely cut ourselves off from society in some sort of Luddite-inspired rebellion. Instead, a Heideggerian-inspired approach to online surveillance based in *Eigentlichkeit* is one in which we "choose to choose" (Heidegger, 1962: 314) our level of comfort when given an option of submitting to online surveillance. For some of us, this may entail seeking alternative, non-digitised technologies that sacrifice some level of convenience in order to retain a greater level of privacy, as Polt (2015) outlined so well in *The Typewriter Revolution*.

Notably, Heidegger does not understand this notion of choosing to choose as related to any sort of ethical stance. It's not as if those who blindly submit to online surveillance are somehow morally "worse" than those who practice more diligence. Heidegger (1998a) insists that his interest is in ontology (the study of being), not ethics. This makes his thought only so helpful in thinking through the issue of online surveillance, as there are clearly ethical implications involved in the pervasive power of this practice. I think we should pay heed to Nietzsche's (1967: §244) claim that "every high degree of power involves *freedom* from good and evil [emphasis original]". Thinking through the power dynamics involved in the asymmetry of information used as a form of control noted by Wark (2019), and discussed above, brings us to the realm of ethics, as those who control the information may be tempted to operate at a level that Nietzsche (1966) would refer to as "beyond good and evil" and thus leverage their power advantage to exploit humans by manipulating human behaviour. Zuboff (2019: 346) crystallises the ethical situation by arguing that "*an information civilization shaped by surveillance capitalism will thrive at the expense of human nature and threatens to cost us our humanity* [emphasis original]". Where then, should we turn to think through this new ethical terrain? I think the most obvious answer to this question lies in the philosophy of Immanuel Kant, who made respecting humanity [*Menschlichkeit*] the core of his ethical system.

Heeding humanity

Like Foucault and Heidegger, Kant lived long before the digital information age and indeed lived much more sheltered a life than either of them. He was born and died in Königsberg, Prussia, and he never ventured far beyond that city's walls. Having lived from 1724 to 1804, Kant died 40 years before the invention of the telegraph and thus would have never dreamt of the current ethical challenges we face in the global and digital information age. Nevertheless, in *Groundwork for the Metaphysics of Morals*, Kant (2002: 7–8) engaged in "the search for and establishment of the supreme principle of morality", which he called "the categorical imperative" and argued that "from this one imperative all imperatives of duty can be derived" (Kant, 2002: 37). Thus, any ethical question as to what obligations we have to one another as rational beings – our duties to each other who fall in the category of rational beings – can be approached from the perspective of Kant's categorical imperative, including questions of online surveillance. Indeed, Richard Herschel and Virginia Miori (2017: 34) have argued that "Big Data is problematic for Kantian beliefs because the actions associated with Big Data challenge the rights and fair treatment of the individual".

Kant argues that there are two types of entities in the world: things and persons. Whereas things can be assigned a price and treated as a mere means to an end, persons have autonomy, which is "the ground of the dignity of the human and of every rational nature" (Kant, 2002: 54). The word "autonomy" stems from the ancient Greek word *autonomos*, a name assigned to political communities that were self-governed or independent instead of being under the governance of another state (*auto* means "self" and *nomos* means "law"). Kant was the first philosopher to apply the concept of autonomy to individuals in emphasising the moral importance of respecting a person's ability to choose one's life in accordance with one's interests. In fact, his self-proclaimed motto of the Enlightenment was "*Sapere aude*! Have the courage to use your own reason!" (Kant, 1963: 3). Because of our ability to give ourselves laws and live in accordance with them, Kant (2002: 46) argued that "*rational nature exists as* [*an*] *end in itself* [emphasis original]", which prompts him to provide what has come to be called the humanity formulation of the categorical imperative: "Act so that you use humanity, as much in your own person as in the person of every other, always at the same time as [an] end and never merely as [a] means" (Kant, 2002: 47). Essentially, this formulation of the categorical imperative tells us that it is wrong to treat persons as mere things to be manipulated to serve our own interests; to do so is to disrespect human nature, which he referred to as our humanity [*Menschlichkeit*].

The Kant scholar Martin Schönfeld provides a helpful analysis of the humanity formulation of the categorical imperative by interpreting it as both a description of what it means to *be* human and a prescription as to how we ought to treat humans:

> We ought to treat humans as ends because they really are ends. That is to say, humans are self-directed, goal-oriented, and highly self-determined living beings, compared to other species on the planet. In comparison, humans are the best embodiment of autonomy. No other species enjoys the degree of freedom of action we do. In this sense, humans are ends. (Schönfeld, 2010: 10)

Kant's understanding that the human capacity to self-determine our lives has moral implications as to how to treat them is a departure from a common theme in Western philosophy from the time of David Hume, one of his prominent predecessors. Since Hume, many philosophers in the Western tradition have been influenced by what is commonly referred to as "Hume's guillotine", that is, the claim that we need to separate statements about the way the world is from the way the world ought to be and that descriptive claims have no bearing on prescriptive claims. Hume (2000: 300) argued that, as compared to *is* or *is not*, "*ought* or *ought not*, expresses some new relation or affirmation" and thus it is "inconceivable how this new relation can be a deduction from [*is* or *is not*], which are entirely different from it [emphasis original]". While Kant (2004:10) famously credited Hume for awakening him from his "dogmatic slumber" – thus acknowledging Hume's influence on his thought – he did not agree with the proposition that the way the world is has no bearing on the way the world ought to be as espoused in Hume's guillotine, since he clearly thought that the fact that humans have a rational nature automatically entailed a moral obligation to respect it. This is why it makes perfect sense to Kant (1963: 7) to speak, for instance, of "crimes against human nature".

In applying Kant's ethics to online surveillance, the first question that must be addressed is what we mean by the word "person". Kant (2002) argued that any rational entity is a person. He explicitly ties rationality to the ability to give oneself laws and act in accordance with them; thus, you and I are persons, but Kant (1963: 86) also explicitly labelled a state as "a moral person". From a Kantian lens, this means that individuals have an obligation to respect each other's autonomy but also that the state has an obligation to respect the autonomy of its citizens, and vice versa. What other entities might qualify as a person? Noam Chomsky (2012: 41) noted that many states "broaden the category of persons to include corporate entities, which now have rights way beyond human beings", and he considered corporate personhood a "gross distortion [of] the concept of person" (Chomsky, 2012: 46). It is beyond the scope of this chapter to elaborate on whether Chomsky is right, but we can certainly entertain the notion that corporations like Google and Amazon are persons, at least under Kant's definition, since they are rational entities in that they have the ability to give themselves laws and act in accordance with them. Although it is human persons making decisions in a corporate entity, those decisions are made on behalf of the corporation and in accordance with its overall interests, as determined by stakeholders. Thus, the corporation functions as a person in a similar fashion as a government acts as a person in the Kantian framework. In her commentary on the instrumentarian power of online surveillance, Zuboff (2019: 17) warned of human beings becoming "the objects of a technologically advanced and increasingly inescapable raw-material-extraction operation" through online surveillance. In Kantian language, the risk is that individual persons are treated as mere means by corporations for the sake of profit, or by governments for the sake of control.

Before we can navigate that ethical terrain, we need to get some clarity as to what it means to be an individual person in the digital age. In his influential 1964 book, *Understanding Media*, Marshall McLuhan (1964: 7) argued that “the personal and social consequences of any medium – that is, of any extension of ourselves – result from the new scale that is introduced into our affairs by each extension of ourselves, or by any new technology”. Under a McLuhanian conception, we can understand our digital footprint – that is, the trail of data created by any device we use that is tied to the Internet – as an extension of ourselves. McLuhan (1964: 4) noted that “whether the extension of consciousness, so long sought by advertisers for specific products, will be ‘a good thing’ is a question that admits of a wide solution”. There are, of course, benefits to the digital information age. For example, biometric data ensures a greater level of accuracy in terms of authenticating persons, which can prove beneficial in the realms of security and criminal justice. Real-time data analytics tied to learning management systems in the realm of academia provide faculty members like myself valuable information to improve student academic performance. We could proliferate many more examples of the benefits of data analytics and online surveillance techniques. At the same time, however, there are risks involved in these techniques when they are pushed to the extreme, due to the asymmetrical information and thus asymmetrical power dynamic involved; indeed, McLuhan (1964: 68) recognised that “once we have surrendered our senses and nervous systems to the private manipulation of those who would try to benefit from taking a lease on our eyes and ears and nerves, we don’t really have any rights left”. There are obvious risks not only when the wrong people get access to information, as in data breaches in which things do not go as planned, but also when the system *is* functioning as planned, since there is potential that corporations or governments will exploit the asymmetry of power noted by Wark (2019) and thus disrespect fundamental human rights.

Autonomous ends

The central question from a Kantian perspective is whether persons are being treated as ends in themselves, thereby respecting their autonomy and heeding their humanity, or whether they are being treated as mere means and thus being exploited. This question requires philosophical reflection regarding the relationships between 1) individual persons and governments, 2) individual persons and corporations, and 3) governments and corporations. To close this chapter, I comment briefly on these three types of relationships.

Regarding relationships between individual persons and governments, Kant’s (1963: 7) claim that “the touchstone of everything that can be concluded as a law for a people lies in the question whether the people could have imposed such a law on itself” is highly relevant. He believed that “men work themselves gradually out of barbarity if only intentional artifices are not made to hold them in it” (Kant, 1963: 9) and argued explicitly that the government should aspire "to treat men [...] in accordance with their dignity" (Kant, 1963: 10). One way to alleviate the potential of exploitation of power on the part of the government towards its citizens is to ensure that individual citizens have a genuine voice regarding which laws ought to govern the country. When government bodies pass legislation without the consent of their citizens, we are right to be suspicious of whether this fundamental principle of respecting human dignity is being put at risk. In my home country of the US, the federal government rapidly passed The Patriot Act a mere 45 days after the terrorist attack on 11 September 2001 in the name of national security, a law that heavily expanded governmental authority to utilise online surveillance on its citizens. In commenting on this, Chomsky (2002: para. 32) has argued:

> [The American government used] this opportunity to try to protect state power from public scrutiny, [which is] part of trying to make the public more obedient and submissive [...]. They would like more control over people, more surveillance, more obedience, more fear, general marginalization. [...] The way you can get away with that [is by ...] ram[ming] through policies you know the public is opposed to.

If we apply Kant's ethics to this situation, it is clear that the American government's unilateral passing of The Patriot Act in a time of crisis without input from the public is unethical, as it does not respect the autonomy of its citizens, especially since the law entailed increasing the power asymmetry between the government and its citizens in favour of the government. As a general Kantian rule of thumb, the state has an obligation to respect the autonomy of its citizens and allow them to choose their lives in accordance with their interests, provided those interests do not place other citizens in danger. While policies can be put in place to limit autonomy given certain contexts (e.g., implementing mask mandates during a pandemic) such policies should be guided by public discourse and not unilaterally implemented by the government, if we are truly respecting individual autonomy.

Regarding the second relationship between individual persons and corporations, the most ethically problematic aspect from a Kantian perspective, to my mind at least, is the potential of behavioural manipulation that Zuboff (2019) outlined, noted above. While I am explicitly trying to move beyond the Orwellian understanding of surveillance in this chapter, we should be reminded of Orwell's (1950: 220) warning of the power "in tearing human minds to pieces and putting them together again in new shapes of your own choosing". In speaking of human beings, Kant (1963: 141) once said that "we are dealing with beings that act freely, to whom, it is true, what they ought to do may be dictated in advance, but of whom it may not be predicted what they will do". The normalisation of data collection tied to data analytics has the capability of erasing some of the surprise elements involved in predicting future human behaviour noted by Kant, as the pervasiveness of online surveillance allows corporations access not only to persons' preferences but to many of their everyday behaviours. Corporations can then use that information to influence future behaviour so that it aligns with their corporate interests through artificial intelligence–driven algorithms, such as recommendation engines. We can understand these as acts of digital nudging (Weinmann et al., 2016). Richard Thaler, who won the Nobel Memorial Prize in Economic Sciences in 2017 for his work in behavioural economics, argued that nudging helps people make better decisions without forcing certain outcomes upon anyone (Thaler et al., 2010). If individuals are simply presented with personalised options based on their past behaviour collected and analysed by the corporation-approved algorithm, we can situate this as an ethical act, since the corporation is still respecting the autonomy of the individual. There is, however, the potential that a corporation may provide information to an individual to trick them into thinking they are making an autonomous choice, exploiting a tendency towards fallacious reasoning that it has discovered through behavioural analytics; this would clearly be an unethical act. We can understand such tactics as acts of interpellation, which Louis Althusser (1971) defined as acts in which individuals are tricked into thinking that they are acting upon their own interests but in fact are being manipulated to serve the interests of others. I have argued that direct-to-consumer pharmaceutical advertising practices in the US already include acts of interpellation that undermine the autonomy of individuals, particularly through their use of fallacious reasoning techniques, including, for example, the common technique of showcasing positive visual cues while verbalising risks and side effects, thus exploiting the human tendency to focus on the visual over the verbal when the content is discordant (Rentmeester, 2022a). If online surveillance techniques on the part of corporations lead to acts of interpellation upon consumers, corporations are treating individuals as mere means to ends and thus disrespecting human dignity.

Regarding the relationship between governments and corporations, it is clear that governmental regulation varies widely from country to country. While my home country of the US still operates on somewhat of an "anything goes" or "wild, wild west" sort of model, the European Union's passing of the General Data Protection Regulation (GDPR) in 2018 has been shown to have "successfully met its objections of strengthening the protection of the individual's right to personal data protection" (Kuner et al., 2021: 9). The US has been famously labelled a corporatocracy by Jeffrey Sachs (2012), who examined the problematic ethical implications of the undue influence of corporate power on government to the detriment of its citizens. If we are to distinguish citizens, corporations, and governments as distinct persons – at least in the Kantian sense – and keep in mind the asymmetry of power between corporations and citizens, as well as between governments and citizens, it is clear that the government must play some role in regulating the avenues that corporations can utilise via online surveillance to exploit its citizens, especially given the pervasive power of this practice noted above. Kant (1963: 128) argued that "the rights of men must be held sacred, however much sacrifice it may cost the ruling power". The most basic right of humans from a Kantian perspective is the right to autonomy since it is tied to human nature. Basic principles in the GDPR that minimally reflect a respect for the right to autonomy include mandating corporations to 1) ask permission and gain consent for the collection and use of personal data; 2) design systems with an eye towards privacy and security; and 3) only collect data necessary to the contractual relationship. A societal setup that does not enact any of these protocols, such as the setup we currently have in the US, allows for too much potential risk to be placed upon individual persons by corporations, given the power asymmetry. Thus, the government has a responsibility to enact such measures upon corporations if it is truly respecting the right to autonomy of its individual citizens.

Conclusion

Using various figures in the history of philosophy, most prominently Foucault, Heidegger, and Kant, I have tried to think through the pervasive power involved in online surveillance, how individuals can respond to but not escape such power through an intentional stance towards it, and what sorts of ethical obligations exist between individual persons, governments, and corporations given that power, if we are to respect the autonomy of persons. Through Foucault, I have argued that online surveillance is embedded in various techniques, pervasively normalised, and is used as a form of control. I have utilised contemporary thinkers, most prominently McKenzie Wark, Shoshana Zuboff, Richard Polt, and Noam Chomsky, to bolster my analysis of some of the power structures that exist between persons in the digital age and the risks involved when those power dynamics are asymmetrical. Through Heidegger, I have argued that his notions of *Gelassenheit* and *Eigentlichkeit* offer a means for individuals to take an intentional stance toward technological devices, at least in some contexts where such a stance is an option. Finally, through Kant, I have argued that his autonomy formulation of the categorical imperative proves helpful in thinking through the basic rights that must be respected for persons in order to respect their autonomy.

I think some of the needed discussion that comes from this analysis should pose genuine questions in the realm of political and corporate policies that need to be taken into consideration and likely adjusted if we are to protect the right to autonomy of persons. Ideally, all relevant stakeholders would have a voice in those discussions, with a particular emphasis on respecting those who have the least power in the relationship and thus are most vulnerable. For those of us who live in places where the power structure is already deeply imbalanced in favour of the government and of corporations, and against the individual person, I think the best advice is to practice diligence in terms of being conscious of the risk involved in willingly submitting to surveillance techniques. In that vein, I end with a quote from Foucault (1984b: 374), who states, “at every moment, step by step, one must confront what one is thinking and saying with what one is doing, with what one is”.

Acknowledgements

I thank Richard Polt and Tony Olson for helpful comments on earlier versions of this chapter.

References

Althusser, L. (1971). *Lenin and philosophy and other essays* (B. Brewster, Trans). Monthly Review Press.

Bacon, F. (1899). *Advancement of learning and novum organum.* The Colonial Press.

Bergen, J. P., & Verbeek, P.-P. (2021). To-do is to be: Foucault, Levinas, and technologically mediated subjectivation. *Philosophy & Technology*, *34*, 325–348. https://doi.org/10.1007/s13347-019-00390-7

Burgess, S., & Rentmeester, C. (2015). Knowing thyself in a contemporary context: A fresh look at Heideggerian authenticity. In H. Pedersen, & M. Altman (Eds.), *Horizons of authenticity in phenomenology, existentialism, and moral psychology: Essays in honor of Charles Guignon* (pp. 31–44). Springer. https://doi.org/10.1007/978-94-017-9442-8

Carabantes, M. (2021). The internet as a Heideggerian paradigm of modern technology: An argument against mythinformation. *AI & Society: Knowledge, Culture and Communication*, *36*, 695–703. https://doi.org/10.1007/s00146-021-01143-x

Chomsky, N. (2002, March 8). On 9-11: Noam Chomsky interview by Nicholas Holt. *Asheville Global Report*. https://chomsky.info/20020308/

Chomsky, N. (2012). *Occupy*. Zuccotti Park Press.

Foucault, M. (1984a). Polemics, politics, and problemizations: An interview with Michel Foucault. In P. Rabinow (Ed.), *The Foucault reader* (pp. 381–390). Pantheon.

Foucault, M. (1984b). Politics and ethics: An interview. In P. Rabinow (Ed.), *The Foucault reader* (pp. 373–380). Pantheon.

Foucault, M. (1984c). Truth and power. In P. Rabinow (Ed.), *The Foucault reader* (pp. 51–75). Pantheon.

Foucault, M. (1990). *The history of sexuality, volume 1: An introduction* (R. Hurley, Trans.). Vintage.

Foucault, M. (1995). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Vintage.

Heidegger, M. (1962). *Being and time* (J. Macquarrie & E. S. Robinson, Trans.). Harper & Row.

Heidegger, M. (1966). *Discourse on thinking* (J. M. Anderson & E. H. Freund, Trans.). Harper & Row.

Heidegger, M. (1969). *Identity and difference* (J. Stambaugh, Trans.). The University of Chicago Press.

Heidegger, M. (1971). *Poetry, language, thought* (A. Hofstadter, Trans.). Harper & Row.

Heidegger, M. (1973). *The end of philosophy* (J. Stambaugh, Trans.). The University of Chicago Press.

Heidegger, M. (1977). *The question concerning technology and other essays* (W. Lovitt, Trans.). Harper & Row.

Heidegger, M. (1998a). Letter on "humanism." (F. A. Capuzzi, Trans.). In W. McNeill (Ed.), *Pathmarks* (pp. 239–276). Cambridge University Press.

Heidegger, M. (1998b). On the essence of truth (J. Sallis, Trans). In W. McNeill (Ed.), *Pathmarks* (pp. 136–154). Cambridge University Press.

Heidegger, M. (2010). *Country path conversations* (B. W. Davis, Trans.). Indiana University Press.

Herschel, R., & Miori, V. M. (2017). Ethics & big data. *Technology in Society*, *49*, 31–36. https://doi.org/10.1016/j.techsoc.2017.03.003

Hume, D. (2000). *A treatise of human nature* (D. F. Norton & M. J. Norton, Eds.). Oxford University Press.

Kant, I. (1963). *On history* (L. W. Beck, Ed.; L. W. Beck, R. E. Anchor, & E. L. Fackenheim, Trans.). Macmillan.

Kant, I. (2002). *Groundwork for the metaphysics of morals* (A. W. Wood, Ed. & Trans.). Yale University Press.

Kant, I. (2004). *Prolegomena to Any future metaphysics that will be able to come forward as science* (G. Hatfield, Trans. & Ed.). Cambridge University Press.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2021). *The EU general data protection regulation: A commentary*. Oxford University Press.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. Polity.

Marcuse, H. (1964). *One-dimensional man: Studies in the ideology of advanced industrial society*. Beacon Press.

McLuhan, M. (1964). *Understanding media: The extensions of man*. Mc-Graw Hill.

Nietzsche, F. (1966). *Beyond good and evil: Prelude to a philosophy of the future* (W. Kaufmann, Trans.). Vintage.

Nietzsche, F. (1967). *The will to power* (W. Kaufmann & R. J. Hollingdale, Trans.; W. Kaufmann, Ed.). Vintage.

Orwell, G. (1950). *1984*. Signet Classics.

Polt, R. (2015). *The typewriter revolution: A typist's companion for the 21st century*. Countryman Press.

Polt, R. (2018). Eidetic eros and the liquidation of the real. In R. Polt, & J. Wittrock (Eds.), *The task of philosophy in the anthropocene: Axial echoes in global space* (pp. 63–83). Rowman & Littlefield International.

Rentmeester, C. (2022a). Pharmaceutical advertising and the subtle subversion of patient autonomy. *The Journal of Medical Humanities*, *43*, 159–168. https://doi.org/10.1007/s10912-020-09633-7

Rentmeester, C. (2022b). Somewhere between Plato and Pinker: A Heideggerian ontology of music. In C. Rentmeester, & J. R. Warren (Eds.), *Heidegger and music* (pp. 235–252). Rowman & Littlefield.

Rosenberg, A., & Westfall, J. (Eds.). (2018). *Foucault and Nietzsche: A critical encounter*. Bloomsbury.

Sachs, J. D. (2012). *The price of civilization: Reawakening American virtue and prosperity*. Random House.

Schönfeld, M. (2010). Metaphysics of sustainability: Kant's categorical imperative. In J. Lee (Ed.), *Sustainability and health* (pp. 1–18). Ria University Press.

Sheehan, T. (2015). *Making sense of Heidegger: A paradigm shift*. Rowman & Littlefield International.

Thaler, R. H., Sunstein, C. R., & Balz, J. P. (2010). Choice architecture. *Social Science Research Network*. http://dx.doi.org/10.2139/ssrn.1583509

Wark, M. (2019). *Capitalism is dead: Is this something worse?* Verso.

Weinmann, M., Schneider, C., & vom Broke, J. (2016). Digital nudging. *Business & Information Systems Engineering*, *58*, 433–436. https://doi.org/10.1007/s12599-016-0453-1

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

Afterword

Future directions for surveillance in practice and research

STEFAN GELFGREN,[I] COPPÉLIE COCQ,[II] JESPER ENBOM,[III] & LARS SAMUELSSON[I]

[I] DEPARTMENT OF HISTORICAL, PHILOSOPHICAL AND RELIGIOUS STUDIES, UMEÅ UNIVERSITY, SWEDEN
[II] HUMLAB, UMEÅ UNIVERSITY, SWEDEN
[III] DEPARTMENT OF CULTURE AND MEDIA STUDIES, UMEÅ UNIVERSITY, SWEDEN

ABSTRACT
The contributions in this book shed light on the complexity of surveillance in a digital age and problematise power relations between the many actors involved in the development and performance of surveillance culture. More and more actors and practices play an increasing role in our contemporary digitalised society, and the chapters show how people negotiate surveillance in their use of digital media, often knowingly leaving digital footprints, and sometimes trying to avoid surveillance. The digital transformation will continue in the foreseeable future. The coordination and analysis of data is viewed by many government agencies, corporations, and other actors as important tools for improving public administration, health, and economic growth. For this development to be legitimate, it is important that hard values, such as technical and legal developments, and soft values, such as ethical and cultural values, are taken into consideration.

KEYWORDS: surveillance culture, digital transformation, counter-practices, data regulation, cybersecurity

Gelfgren, S., Cocq, C., Enbom, J., & Samuelsson, L. (2023). Afterword: Future directions for surveillance in practic and research. In L. Samuelsson, C. Cocq, S. Gelfgren, & J. Enbom (Eds.), *Everyday life in the culture of surveillance* (pp. 205–211). Nordicom, University of Gothenburg. https://doi.org/10.48335/9789188855732-a

Online surveillance through a prism of different traditions and fields

The contributions in this anthology illustrate a broad range of perspectives. Together, they shed light on the complexity of surveillance in a digital age and provide insight into the implications of the surveillance culture we live in. Such an insight is, for instance, how a commonplace practice such as mobile gaming is embedded in an economic model based on the commodification of personal data and the distribution of targeted advertising. Hence, mobile gaming plays a role in dataveillance on a grand scale, and the authors of Chapter 1, Maude Bonenfant, Alexandra Dumont, and Laura Iseut Lafrance St-Martin, observe how a collective habituation contributes to trivialising surveillance. As explained by Shawn Kaplan in Chapter 2, ethical considerations regarding surveillance demonstrate that not only must we acknowledge and conform to a right to privacy, but also articulate a right to obscurity, in order to protect the interests of individuals and the societal interests of liberal democracies (e.g., citizens must be able to engage in protests and political rallies without a looming threat of negative repercussions).

This anthology also stresses the importance of understanding motives and perceptions of individuals. For instance, as Kristina Stenström outlines in Chapter 4, individuals engaged in fertility self-tracking practices are often aware of and appreciate the potential risks involved in these practices but take them to be outweighed by the perceived benefits. While the participants in Stenström's study were critical to, and sometimes concerned about, data collection and sharing, they tended to view the potential sharing of fertility data as something to be expected in a time and culture relying so heavily on data collection. Motives behind, and perceptions of, surveillance are also approached by Lars Samuelsson in Chapter 6, which shows how potential personal gains of being surveilled online do not generally increase the acceptance of such surveillance (among the group of Swedish students he studied). In fact, many seem to be more or less unconditionally opposed to online surveillance. And to the extent that people do differ in their acceptance of surveillance, the difference seems to lie in their general attitude to being surveilled rather than in their approach to ethical reasoning.

Surveillance is reflected in various contexts, as this anthology highlights, for instance, digital influencer marketing, illustrated by Johanna Arnesson and Eric Carlsson in Chapter 3 – both as typically gendered forms of self- and peer-surveillance, and top-down surveillance. In the case of the Swedish influencer industry, gendered social surveillance is an inherent part of influencer culture, and something that both causes conflict and underpins commercial success. Attitudes to surveillance must be understood in relation to this variety of contexts, for instance, in relation to the type of surveillance considered. This is, for instance, illustrated by Rikke Frank Jørgensen in Chapter 5, in which she compares three types of surveillance – CCTV surveillance, monitoring of information exchanged on the Internet, and the collection of information about citizens without their knowledge – and argues that the variations in attitudes towards them can be explained by the different types of exposure they entail and the privacy norms associated with them. In a similar vein, Liisa A. Mäkinen and Johanna Junnila, in Chapter 7, show how young people in Finland tend to contextualise potential audiences with whom their smartphone data could be shared. They illustrate how, in their everyday life, young people consider the protection of their personal information more important in relation to friends and social groups than in relation to organisations, authorities, and commercial entities. Thus, system-level surveillance and data collection often go unnoticed, are overlooked, or purposefully ignored, even though they are constantly happening in the background.

Attitudes, adaptations, and negotiations

As many contributions in this anthology show, individuals are to a great extent aware and conscious of the risks they take when engaging in digital practices. Some of the authors problematise strategies and responses to this. For instance, in Chapter 8, Luise Salte reveals that while the Norwegian social media natives she interviewed continued using social media platforms for social benefits, they implemented protective strategies to circumvent what they perceived as risks. Hence, the benefits are primarily reached by creating private and closed spaces. Spaces outside of such private locations were largely seen as unfit for political and public issue conversations, and even for any actions of which much meaning or opinion may be interpreted. This aspect is also approached by Casey Rentmeester in Chapter 9, where the focus is on the pervasive power involved in online surveillance and how individuals can respond to but not escape such power through an intentional stance towards it – in investigating what sorts of ethical obligations exist between individual persons, governments, and corporations.

The country-specific studies by Jørgensen (Denmark, Chapter 5), Samuelsson (Sweden, Chapter 6), Mäkinen and Junnila (Finland, Chapter 7), and Salte (Norway, Chapter 8), touch upon the fact that attitudes towards surveillance differ. Sometimes surveillance (or data sharing, to use a more neutral expression) is seen as just and fair and sometimes it makes people consciously avoid being surveilled, but often the services offered are too good, too convenient, or too integrated in everyday life to refrain from using them. We can expect it to be increasingly difficult to avoid surveillance as more and more data is created and shared in our everyday life. Many of our gadgets and devices already share data – what is referred to as "smart homes" and the "Internet of things" will connect our phone with the car, the refrigerator, and the media consumption unit (phone, computer, Apple TV, Playstation, etc.), and so on, and keep track of our lives for our convenience. Where this will end is yet to be seen.

Two intertwined developments

As a whole, the contributions in this volume problematise power relations between the many actors involved in the development and performance of surveillance culture. Together, they highlight at least two different threads of development: first, those we have not yet seen the result of, and which will spur new societal dilemmas, and second, new research questions.

First, it is clear how contemporary surveillance culture involves more and more actors and practices. Individuals and their quotidian digital practices, influencers, commercial actors, authorities, and so on, all play an increasing role in contemporary surveillance culture. Power relations become increasingly complex and opaque, and we are all intertwined (even embedded) in a web of surveillance practices with non-discernible actors. This leads to a second line of overall development that several chapters in this book touch upon, namely the increasing need and urge to handle the all-intrusive surveillance. In, for example, the cases dealing with the Nordic countries, it becomes clear how people negotiate surveillance: They use digital media, they know they leave digital footprints, and they know their data is used for various forms of surveillance – and they find it problematic and try to avoid it by using different counter-practices.

These two developments are intertwined, and illustrated by the different contributions in this book. However, this is something we, expectedly, have only seen the beginning of. The anticipated digital transition of society will drive this development forward. The expected increase of use of data by companies and authorities will have an effect on how people view their data, and their possible involvement in the use of data. Therefore, we can expect these discussions to continue in the near future.

This anthology has largely studied and emphasised surveillance culture from the perspective of individuals and "ordinary people". However, countermeasures to regulate surveillance and data sharing and usage are also taken on a macro level, for example, by national authorities or the European Union. One major development regarding personal data and surveillance culture is the strengthened regulation in the EU. The General Data Protection Regulation (GDPR) was decided in 2016 and implemented in May 2018. The purpose was to protect the personal data of individuals but also to clarify rules for corporations and public bodies active in the EU member states (European Union, n.d.-a).

In July 2022, the European Parliament furthermore approved the Digital Services Act (DSA) along with the Digital Markets Act (DMA), and on 4

October 2022, the European Council gave the regulations their final approval (European Union, n.d.-b). The aim of DSA and DMA is to safeguard users of digital services and to create fairer business conditions – in other words, regulate the unrestricted use of data. Corporations providing digital services, for example, social networks and content-sharing platforms, will be banned from using certain personal data, including data about ethnicity and political and religious beliefs, for the purpose of online advertising (European Union, n.d.-c). Furthermore, more transparency will be demanded from the online platforms, including how they use algorithms for recommendations. All these regulation measures are likely to change the conditions for the existing surveillance capitalism in Europe, including the Nordic countries. The short-term as well as long-term consequences of this development will be interesting to observe and should be a fruitful avenue for further research studies, not least because the new regulations stipulate "access for researchers to key data of the largest platforms and search engines" (European Union, n.d.-c).

Future directions: Surveillance in practice and research

This anthology also leaves several dimensions of surveillance culture unaddressed. For example, knowledge about generational aspects regarding attitudes to surveillance is insufficient. Research about the use and impact of data among the elderly is scarce, and if several chapters in this volume investigate surveillance culture among youngsters, none have studied the equivalent among the oldest generation. However, for instance, the report *The Swedes and the Internet 2021* pointed to the risk of digital exclusion when "every fifth pensioner does not use the internet in 2021" (Swedish Internet Foundation, 2021). The same report also stated that the feeling of insecurity is a reason for not using the Internet daily, and that the elderly are most worried about but also least exposed to online fraud attempts. This underscores the importance of understanding attitudes to Internet use (such as a feeling of vulnerability and insecurity) and data use in order to resist digital exclusion.

Similar patterns can also be seen in relation to people with disabilities, particularly cognitive disabilities. The diversity and complexity of digital literacy for groups with disabilities, and their social surroundings, must be acknowledged. There are concerns regarding this group's vulnerability in a context of surveillance culture, or, rather, their possibility to counter, challenge or resist misuse of their data (Gelfgren et al., 2022). This is also a marginalised group in relation to surveillance studies, and further research on this aspect is therefore relevant.

Since this anthology focuses on the Nordic countries, certain forms of surveillance are understandably not included. Studies in various contexts outside the European and Anglo-Saxon world, for instance, are needed in order to nuance the Western-centric perspectives of this book. More cultural perspectives are needed to understand the full nuances and particularities of surveillance. In addition, the political situation in a society affects the use and perception of surveillance. In totalitarian states, for example, digital communication can be a means for rebellion, but can also be turned toward the users as a means of oppression. This is not covered in this book either.

Neither are the more explicitly data- and surveillance-hesitant groups. To be hesitant and sceptical of surveillance is of course not new. However, in the wake of the Covid-19 pandemic, we could see how "data-critical groups" were formed on a larger basis – groups who are concerned and critical to how our data is gathered and used by companies and authorities, and now air their voices in public.

Surveillance, and the related issues of data management, is indeed intrinsically intertwined with the contemporary world and our everyday lives. Today, there is a political and economical discourse to push the digital transformation forward. The coordination and analysis of data, and technologies such as facial recognition and GPS tracking, give high hopes to save natural resources, provide health and wealth to the people, and gain economical growth. How these future processes will fold out in the long run is still to be discovered. For the digital transformation to be a success, it must be implemented in a legitimate way and built on the trust of citizens.

Here, we can also see how different attitudes and experiences toward digital development play a role in future directions. On a global scale, three different approaches toward future directions are noticeable, boiled down to "state control in China, citizen voice in Europe, and business practices in America", in reference to Bal and Gil (2020), here in relation to artificial intelligence. While China seeks to develop artificial intelligence centrally by the state, the US puts the initiative to develop it in the hands of businesses, and Europe tries to find a middle way, also involving concerns about citizens. From a European perspective, it is considered important to strengthen both European industrial competitiveness and address concerns over data sovereignty. There are initiatives, from the EU top level, to both juridically restrict the possibility to freely and unlimitedly use European data outside Europe (referring back to the related discussion on GDPR), and to develop its own software (e.g., social media platforms) and hardware (e.g., chips and exascale computers). As mentioned above, business conditions and fair competition have been central concerns behind the adaptation of DSA and DMA. On the basis of data sovereignty and cybersecurity, the role of Chinese technology has been discussed, for example, in relation to the social media app TikTok, or Huawei's role on the cell phone and 5G market, as well as the role of American media platforms such as Google, Facebook, and Apple (see, e.g., Farrand & Carrapico, 2022; Floridi, 2020; Lewis, 2020). This has bearing on future developments of everyday surveillance – in Europe, but also elsewhere. How this will pan out over the next few years we must wait and see (and as the different contributions in the book show – we will also be engaged in).

The digital transformation will continue in the foreseeable future, if nothing really disruptive occurs, and in order to be the intended success story, both hard values, such as technical and legal developments, and soft values, such as ethical and cultural values, must go hand in hand. So, the issue regarding everyday practices in relation to the culture of surveillance will prevail, and depending on how the development goes, new questions and new issues to tackle will arise. Therefore, we, the editors, see this book as a continuation of asking questions and raising awareness of these issues – in contemporary society, and for the near future.

References

Bal, R., & Gill, I. S. (2020). Policy approaches to artificial intelligence based technologies in China, European Union and the United States. *Duke Global Working Paper Series No. 26.* http://dx.doi.org/10.2139/ssrn.3699640

European Union. (n.d.-a). *Data protection in the EU: The general data protection regulation (gdpr), the data protection law enforcement directive and other rules concerning the protection of personal data.* https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

European Union. (n.d.-b). *The digital services act package.* https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

European Union. (n.d.-c). *The digital services act: Ensuring a safe and accountable online environment.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*, 369–378. https://doi.org/10.1007/s13347-020-00423-6

Gelfgren, S., Ineland, J., & Cocq, C. (2022). Social media and disability advocacy organizations: Caught between hopes and realities. *Disability & Society*, *37*(7), 1085–1106. https://doi.org/10.1080/09687599.2020.1867069

Lewis, J. A. (2020, October 26). *Digital sovereignty in a time of conflict.* Observer Research Foundation. https://www.orfonline.org/expert-speak/digital-sovereignty-in-a-time-of-conflict/

The Swedish Internet Foundation. (2021). *Svenskarna och internet 2021* [*The Swedes and the Internet 2021*]. https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2021

Over the recent decades, the possibilities to surveil people have increased and been refined with the ongoing digital transformation of society. Surveillance can now go in any direction, and various forms of online surveillance saturate most people's lives, which are increasingly lived in digital environments.

To understand this situation and nuance the contemporary discussions about surveillance – not least in the highly digitalised context of the Nordic countries – we must adopt cultural and ethical perspectives in studying people's attitudes, motives, and behaviours. The "culture of surveillance", to borrow David Lyon's term, is a culture where questions about privacy and publicness, and rights and benefits, are once again brought to the fore.

This anthology takes up this challenge, with contributions from a variety of disciplinary and theoretical frameworks that discuss and shed light on the complexity of contemporary surveillance and thus problematise power relations between the many actors involved in the development and performance of surveillance culture. The contributions highlight how more and more actors and practices play a part in our increasingly digitalised society.

The book is an outcome of the research project "iAccept: Soft surveillance – between acceptance and resistance", financed by the Marcus and Amalia Wallenberg Foundation. The anthology's editors are project members, all based at Umeå University, Sweden: Lars Samuelsson, associate professor of philosophy; Coppélie Cocq, professor of Sámi studies and digital humanities; Stefan Gelfgren, associate professor of sociology of religion; and Jesper Enbom, associate professor of media studies.

NORDICOM

UNIVERSITY OF
GOTHENBURG

Nordic Council
of Ministers

Nordicom is a centre for Nordic media research at the University of Gothenburg, supported by the Nordic Council of Ministers.

ISBN 978-91-88855-72-5

9 789188 855725