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