Spring 4-29-2020

Governmental Surveillance - The balance between security and privacy

Marie Eneman
University of Gothenburg, marie.eneman@gu.se

Jan Ljungberg
University of Gothenburg, jan.ljungberg@ait.gu.se

Bertil Rolandsson
University of Gothenburg, bertil.rolandsson@gu.se

Dick Stenmark
University of Gothenburg, dick.stenmark@ait.gu.se

Governmental Surveillance
- The balance between security and privacy

Marie Eneman, University of Gothenburg, marie.eneman@gu.se
Jan Ljungberg, University of Gothenburg, jan.ljungberg@ait.gu.se
Bertil Rolandsson, University of Gothenburg, bertil.rolandsson@gu.se
Dick Stenmark, University of Gothenburg, dick.stenmark@ait.gu.se

Abstract

The increased digitalisation of society and recent developments in AI is laying the ground for surveillance capabilities of a magnitude we have not seen before. Surveillance can be conducted by several different actors in society, this project focuses on the Swedish police currently using a large ensemble of surveillance technologies. Earlier this year, significant legislative changes governing the police authorities use of digital surveillance were enacted. These changes mean that the police now have been given an extended mandate to use digital surveillance as part of their professional practice, which places demands on balanced decisions and informed responsibility. On the one hand, the police have an interest to use digital surveillance to increase efficiency and security in society; on the other hand, the police must balance their interests with citizen's so-called integrity-interests and right to privacy. This study will therefore examine to what extent the Swedish Police Authority pay attention to questions such as integrity and privacy when introducing digital surveillance. The study is guided by the following questions: (i) What opportunities can be related to the implementation and use of digital surveillance in police work? (ii) What kind of challenges do the increasing use of digital surveillance create between organisational governance, police officers' work practice, and the integrity of citizens - and how do the police tackle these challenges? Theoretically, we draw on the established research fields on surveillance and privacy and empirically this study is designed as a qualitative study of the Swedish Police as our main case.

Keywords: Digital surveillance, law change, public authorities, Swedish Police, security, privacy, qualitative study

1. Introduction

Surveillance is not a new phenomenon in society, but the increased digitalisation of society and recent developments in Artificial Intelligence (AI) and machine learning is laying the ground for powerful surveillance capabilities of a magnitude we have not seen before (European Commission, 2020). One of the most significant changes, due to the continued digital development, is that today's surveillance systems become more powerful, subtler, further automated and large-scale in their collection of sharing and storage of data, often also ubiquitous and difficult to detect (Matzner, 2016). It has been argued that today's digital technologies enable much more efficient control of the citizens than what Georg Orwell predicted in his dystopian classic '1984' (Murray, 2016). Literature has acknowledged the tension between, on the one hand, society's desire and need for security and, on the other hand, the individual's right to integrity and privacy (Helm and Seubert, 2020; Solove, 2011). The growing public fear of acts of terrorism following the 9/11 paired with the continuous technological development, threatens to tilt this balance further over towards security. Law proposals never passed due to their controversial nature were implemented overnight in the wake of the terrorist attacks during the early years of the new millennium (Lyon, 2015). A more recent illustration can be found in relation to the spread of the Covid-19 pandemic, where public authorities in various European countries quickly extended their mandate to use digital technologies to monitor citizens.

Surveillance can be conducted by a number of different actors and also on different levels in society. This study focuses upon digital surveillance conducted by public authorities and a central actor in this context is police authorities currently using a large number of surveillance technologies. Technology plays a key role in police work with expectations of improved effectiveness and legitimacy (Manning, 2016). Emerging technologies can be described as extending police officers' capacity to see, hear, communicate, record, recognize, and analyse (Haggerty and Ericson, 1999, Eneman et al, 2018). Information gathering about human behavior and environment is a fundamental component in police work and digital technologies can, from a police perspective, be seen as ideal for collecting, process and store large volumes of information. In this study, we are focusing upon police authorities use of digital surveillance technologies, since many police authorities world-wide currently are using, and increasingly so, a large ensemble of surveillance technologies. This includes stationary surveillance systems (e.g., CCTV), body-worn cameras, cameras in cars, drones and a variety of sensors and more. In addition, the most recent developments in algorithms and artificial intelligence advances the analytical capabilities in surveillance further, for example by enabling large-scale face and motion recognition, with major expectations on improved effectiveness, security, transparency and legitimacy. On the one hand, these surveillance technologies are described as tools with expectations of improving effectiveness and security in society, on the other hand the technologies are associated with concern of threats to individuals' integrity and privacy since large volumes of personal and sensitive data easily can be collected and processed both within and between systems. To what extent public authorities acknowledge this duality remains largely unknown.

This study is empirically based on concrete initiatives taken by the Swedish Police Authority introduction of digital surveillance. Swedish public authorities, and especially the police, are surrounded and regulated by legislations, statutes and

policies. To ensure and improve the protection of individuals' personal data in todays' digital society, a number of legislations and statutes have been created and implemented, both on national (e.g. The Swedish Camera Surveillance Act (2018:1200)) level and on EU-level (e.g. The General Data Protection Regulation GDPR). The Swedish legislation - The Camera Surveillance Act (2018:1200) has recently been subject to some significant changes. According to the initial legislation enacted 2018, the Swedish police had to apply for permission at the Swedish Data Protection Authority before they were allowed to implement surveillance technologies as part of police work (body-worn cameras are an exception due to the mobility aspect). The new legislative change, enacted January 1, 2020, have however removed the old requirement of applying for permission at the Swedish Data Protection Authority. This means that the Swedish police now has been given an extended mandate (and power) to make the decisions regarding the implementation and use of digital surveillance. Thus, this means that they now are responsible for the process of assessing the different interests involved. They have to consider the police authorities' interest in and need to implement digital surveillance in parallel with considering citizen's so-called integrity-interest. This recent development is highly relevant for this study due to the risk of setbacks regarding privacy protection at a societal level.

Purpose and research questions

As described, the Swedish police is currently using an assemblage of digital surveillance technologies with high expectations on improved effectiveness and security. The increased use of surveillance technologies will doubtlessly affect society in multiple ways, with opportunities as well as challenges and foreseen as well as unforeseen consequences. Digital surveillance is already used in a variety of contexts and is expected to be further extended. Nevertheless, a range of highly important questions concerning implementation, organisation, use, governance/regulation, management and storage of collected data and aspects related to privacy remain to be investigated (Mateescu et al., 2016; The Swedish Data Protection Authority, 2020). The empirical starting point and the main case for this study is (as mentioned above) the Swedish police, but other related public authorities, such as The Swedish Data Protection Authority, The Ministry of Justice, The Swedish Prosecution Authority, The Crime Prevention Council and The Swedish Civil Contingencies, will also be included.

With this as a background, this study will explore the following two research questions: (i) What opportunities can be related to the implementation and use of digital surveillance in police work? (ii) What kind of challenges do the increasing use of digital surveillance create between organisational governance, police officers' work practice, and the integrity of citizens - and how do the police tackle these challenges? Theoretically, we draw on the established research fields on surveillance and privacy and empirically this study is designed as a qualitative study of the Swedish Police as our main case.

2. Theoretical foundations

Surveillance

The term surveillance (from the French verb meaning to watch over) refers to processes with a particular interest in watching human behavior that go far beyond common curiosity (Lyon, 2015). Surveillance is the focused, systematic and routine attention to personal details for certain purposes, its attention is mainly directed to individuals (Matzner, 2016). The focus on individuals, human behavior and personal details should not be understood as something random or spontaneous, it is deliberate (Lyon, 2018; Matzner, 2016). Surveillance has been recognised as a difficult concept to theorise because of its broad and slippery nature, and the fact that it refers to everything from practices, processes, uses, and contexts, to technology, renders it not easily amenable to generalizing statements (Haggerty and Ericson, 2006). Nonetheless, as Haggerty et al. (2011) explain, "it is undeniable that we are in the midst of a fundamental transformation in the scope, intensity and functioning of surveillance, something that makes the task of theorizing surveillance in all domains all the more pressing" (p. 233-234).

One of the most unparalleled metaphors of the power of surveillance in our contemporary society is panopticon - originally an architecture design developed by Bentham as a special surveillance tower for a prison (Foucault, 1979). This architecture consists of a central visible surveillance tower and a courtyard surrounded by an outer ring of cells (Willcocks, 2004). The visibility aspect is of vital importance in the panopticon design, since it constantly reminds the prisoners of the possibility of being observed (Foucault, 1979). The design is based upon the principle that the few guards in the tower could watch the many prisoners in the cells, while the observed could not communicate with each other, nor see the observers, but are constantly aware of the risk of being monitored by the guards. With this design, surveillance became automated and depersonalized as the identity of the observer remains hidden (Lyon, 2015). Foucault (1979) reinvented the concept of panopticon as a metaphor for modern disciplinary societies. Panopticon can be seen as the illusion of constant surveillance, since the prisoners are constantly aware of the risk of being monitored regardless if they are monitored or not (Foucault, 1979; Willcocks, 2004). The feeling of constant surveillance creates a permanent panopticon, where the prisoners act as if they are constantly monitored. The panopticon design constitutes a power mechanism that aims to control and discipline the prisoners' behaviours (Willcocks, 2004). As the individual prisoners fear that they might be watched, and fear punishment for transgressions, they internalise rules (Foucault 1979). Through the use of digital technologies, the surveillance capabilities have been expanded and further automated, not least since the technologies enable many processes and tasks to be performed at the same tie, can be used to large-scale collection and storage of data also allows for data to rapidly flow within and between different systems (Bauman & Lyon, 2013). The issue of visibility is a significant difference between the original panopticon and digital surveillance technologies since todays surveillance systems often are concealed in the environment and thus invisible for individuals in society (Lyon, 2018). Even that panopticon is a strong metaphor to conceptualize and understand surveillance practices it has been subject for certain critique for its potential limitations to adequately understand contemporary technological societies (Zuboff, 2019). The critique has mainly questioned whether researchers should move beyond panopticon

when studying surveillance in modern society based upon the argument that the concept may not cover and reflect all aspects of new technologies (Haggerty, 2006). However, despite the critique, the concept of panopticon is still central and widely used in surveillance studies in contemporary societies (Lyon, 2018; Eneman 2009).

As described above in the introduction, surveillance is not a new phenomenon, the increased digitalization of society has however profoundly altered the surveillance capabilities. One of the most significant changes is that digital technology enables surveillance system to become more powerful, further automated, subtle and can be used for large-scale collection and storage of data (Matzner, 2016). A consequence of this is that individuals are not always aware of when being exposed to surveillance, which could be seen as a serious threat to individuals' privacy (Whitaker, 1999). Another effect is that large volumes of information about individuals' behavior and personal details is collected, which means that material consisting of personal information must be managed and stored within the organisation in line with applicable law (Eneman, et al 2018).

Privacy

Concern regarding surveillance in modern societies have mainly focused upon the issue of privacy. Like surveillance, privacy is a concept difficult to capture, and researchers of privacy have struggled with defining this ambiguous term. Originally, privacy was defined as the right to be let alone, but in our contemporary digital society, the term privacy is often understood and defined as the right to control information about oneself (Helm and Seubert, 2020). Solove (2005) argues that most discussions of privacy appeal to people's fears and anxieties, but commentators often fail to translate those instincts into a reasoned, well-articulated account of why privacy problems are harmful. Therefore, it is unclear precisely what people mean when they claim that privacy should be protected. To remedy this situation, Solove has suggested a taxonomy of privacy that acknowledges that privacy is not a unitary concept with a uniform value, which is unvarying across different situations. Instead, privacy in Solove's taxonomy can be understood as protection from a cluster of related activities that impinge upon people in related ways, and the taxonomy organises these problematic activities into four overarching groups or categories:

(1) Information collection. Information is collected via surveillance or interrogation and creates disruption through the process of gathering information about the subject, often ubiquitously without informed content. Surveillance is the watching of, listening to, or recording of an individual's activities, whereas interrogation consists of various forms of questioning or probing for information. Even if no information is revealed publicly, information collection per se can constitute a breach of privacy.

(2) Information processing. Information processing refers to the storage, manipulation, and use of information that has previously been collected. This includes the aggregation of various pieces of information about a person, and the use of information collected for one purpose for a different purpose without the data subject's consent. It also covers the failure to allow the data subject to know about the information that others have about her and participate in its handling and use.

(3) Information dissemination. Information dissemination is one of the broadest groupings of privacy harms and involves the spreading or transfer of personal data or the threat to do so. This includes activities such as breach of confidentiality or exposure of sensitive material, the revelation of truthful information about a person

that impacts the way others judge her character as well as dissemination of false or misleading information.
(4) Invasion. The fourth and final group of activities involves invasions into people's personal businesses. Invasion harms differ from the harms of information collection, processing, and dissemination because they do not always explicitly involve information. Intrusion may involve invasive acts that disturb one's tranquility of solitude, but also decisional interference that involves the government's incursion into the data subject's private affairs.

The progression from information collection to processing to dissemination is the information moving further and further away from the data subject, making control of these activities increasingly difficult. Invasion, in contrast, progresses toward the data subject and involves impingements directly on the individual. The relationship between these different categories is illustrated in Figure 1.

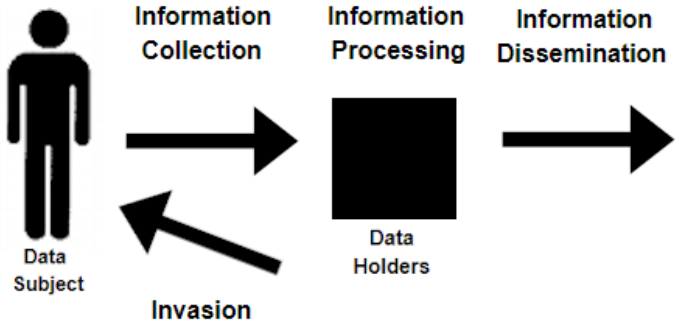

Figure 1. The A taxonomy of privacy (Source: Solove, 2005)

3 Research Design

In our quest to learn how public authorities handle the tension between security and privacy, we will study the Swedish police authority as our main empirical setting and also at later stages include related authorities, e.g., the Ministry of Justice, the Data Protection Authority, the Swedish Prosecution Authority, the Crime Prevention Council and the Swedish Civil Contingencies. The police is a public authority with a broad societal mission aimed at reducing crime and increasing security in society through preventive, interventive, and investigative activities (Manning, 2016). This implies that the police constitutes a concrete case of government work that must relate to a variety of requirements for accountable, legitimate and lawful work (Eneman et al, 2018).

The study is designed as a qualitative study (Silverman, 2018) and we will combine interviews and document studies for collecting empirical material with the ambition to capture different perspectives involved in shaping the digital surveillance practices. We will interview repondents with different interest and involvement in surveillance practices and analyse relevant official documents (e.g. legislation, statutes, policies and more). By combining these two methods, the study will be able to compare

different perspectives on surveillance and form a broad understanding of how public authorities in a western digital society handle the tension between the opportunities with digital surveillance and protecting citizens integrity and privacy. Our primary source of material will be obtained through structured in-depth interviews (Holloway and Jefferson, 2004). We choose to conduct interviews as it is a useful technique for gaining insights into the perceptions, experiences, values, feelings and understanding of individuals, and an understanding how they construct, make sense of and give meaning to their worldviews (Czarniawska, 2008).

In order to understand the digital surveillance practices from several different angels and further capture the broader organisational context, we will also collect and analyse documents that are relevant to the project (Alvesson and Sveningsson, 2008). This can include everything from legislation, policy documents, political debates, proposals, directives to more operational meeting documentation. Through the document studies, the project is given the opportunity to investigate the formalities surrounding the practices where surveillance technologies are involved, and how these practices have been developed and are being developed in a wider institutional and political context. Documents as empirical material can often be a valuable source to better understand the broader organisational context, as organisational systems should be understood on the basis that they do not occur naturally in society but always have a historical and political origin and benefit certain interests at the expense of others (Prior, 2003).

We will conduct analysis and theorising as an integral part throughout the research process (Alvesson and Sveningsson, 2008). When we approach the material, our attention will on patterns, variations and not least the unexpected (Coffey & Atkinson, 1996). In order to ensure that the project is conducted in line with appropriate research ethics we will follow the instructions from the Swedish Ethical Review Authority and the ethical research principles formulated by the Swedish Research Council regarding social science research.

4 Concluding Reflections

This study set out to deepen the knowledge about digital surveillance practices within the police authority in the light of the new extended mandate, caused by the recent law change. We recognize that the police has high expectations related to the introduction of digital surveillance as part of police work, more specifically the expectations refer to increased efficiency and security, as well as strengthen accountability and trust in the police. However, the literature also expresses concerns about threats to citizens' integrity and privacy claiming that hat current privacy measures are insufficient in relation to new powerful technologies (Helm and Seubert, 2020; Solove, 2011). These different expectations imply that the consequences that digital surveillance gives rise to, can be understood both on individual, organisational and societal level, and brings with it both opportunities and dilemmas. In accordance, this study draws on empirical material that reflects how police officers tackle these different challenges related to digital surveillance practices. In particular, we study the balance and tensions between the police authority's interest and need to increase security and citizen's right to integrity and privacy which constitute important democratic values.

We need to understand how these new means for digital surveillance are embedded in different social settings and practices shaped by different social norms in addition to laws. We need more knowledge about how the police and other regulatory authorities approach the use of digital surveillance in relation to expectations on legitimacy and the rule of law. This further highlights the need of regulation and policies focusing both on the use of digital surveillance technologies and the storage and management of the collected data, that often includes both personal data and also personal sensitive data (Matzner, 2016).

Research shows, however, that surveillance technologies develop fast and that the regulative frameworks that try to shape these emerging modes of governmentality are still in their infancy (Murray, 2016). There is thus little guidance for managers and policy makers trying to decide what data is allowed to be collected, under what circumstances, how it can be analysed, how and for how long it can be stored, and who should have access to the data (Eneman et al, 2019). However, surveillance should not only be understood in terms of laws and regulations, but also from a moral and ethical perspective. Not everything that is legal is morally desirable in society and we therefore need to understand all the implications the digital development has on our society. Surveillance conducted at state levels through public authorities is clearly a topical area in need for more research.

We contribute to the theoretical development of digital surveillance by linking to the research fields of surveillance and privacy. The topology suggested by Solove (2005) offers analytical tools to deconstruct privacy in a useful way, and thus allowed us to investigate more easily different aspects of privacy. Our work will continue to provide feedback on the value of the topology and hopefully be able to update, modify, and fine tune it. In future research it would also be interesting to include how citizens respond to the intensified surveillance in society, conducted by regulatory authorities such as the Police. Not least since some researchers argue that surveillance evoke active resistance (Ball, 2006; Eneman, et al 2018). We hope that this paper will provide a catalyst for a continued debate and knowledge development of how public regulative authorities manage the balance of security and privacy when it comes to digital surveillance conducted by public authorities in society.

References

Alvesson, M & Sveningsson, S (2008) Changing organizational culture: Cultural change work in progress, Routledge.

Ball, K (2006) Organisation, surveillance and the body: towards a politics of resistance, in Theorizing surveillance: the panopticon and beyond (ed) David Lyon, Willan Publishing

Bauman, Z & Lyon, D (2013) Liquid Surveillance, Polity Press.

Coffey, A & Atkinson, P (1996) Making sense of qualitative data: Complementary research strategies, SAGE Publications.

Czarniawska, B. (2008), Organizing: how to study it and how to write about it, Qualitative Research in Organizations and Management, Vol. 3 No. 1, pp. 4-20.

Eneman, M., Ljungberg, J., Rolandsson, B., & Stenmark, D (2018) Encountering camera surveillance and accountability at work: case study of the Swedish police, in the Proceeding of the 23rd UK Academy for Information Systems International Conference. Oxford, UK.

Eneman, M (2009) Counter-Surveillance Strategies Adopted by Child Pornographers, in the International Journal of Technology and Human Interaction, Volume 3, pp 1-18.

European Commission, (2020) White Paper: On Artificial Intelligence - A European Approach to Excellence and Trust.

Foucault, M. (1979) Discipline and Punish: The Birth of the Prison, Penguin Books Ltd.

Haggerty, K. D., Wilson, D., & Smith, G. J. (2011). Theorizing surveillance in crime control, Theoretical Criminology, 15(3).

Haggerty, K. D. and Ericson, R. V. (2006) "The New Politics of Surveillance and Visibility", in Haggerty & Ericson (eds.) The New Politics of Surveillance and Visibility, pp. 3–25. Toronto: University of Toronto Press.

Haggerty, K. D. & Ericson, R. V. (1999) The Militarization of Policing in the Information Age, Journal of Political and Military Sociology, 27(2).

Helm & Seubert (2020) Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies,

Hollway, W & Jefferson, T (2004) Doing qualitative research differently, SAGE Publications.

Lyon, D (2015) Surveillance Studies: On Overview, Polity Press.

Lyon, D (2018) The Culture of Surveillance, Polity Press.

Matzner, T (2016) Beyond data as representation: The performativity of Big Data in surveillance. *Surveillance & society* 14(2).

Manning, P.K (2016) *Democratic policing in a changing world*, New York: Routledge Ltd.

Murray, A (2016) Information Technology Law: The Law and Society, Oxford University Press.

Prior, L (2006) Using documents in social research, SAGE Publications.

Silverman, D (2018) Doing Qualitative Research, SAGE Publications Ltd.

Solove, D. J. (2005) A taxonomy of privacy, in University of Pennsylvania Law Review, 15(4).

Solove, D. J. (2011). Nothing to hide: The false tradeoff between privacy and security. Yale University Press.

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

Willcocks, L. (2004) Foucault, Power/Knowledge and Information Systems: Reconstructing the Present In Social Theory and Philosophy for Information Systems. John Wiley & Sons, Ltd.
Wood, D. M., Ball, K., Lyon, D., Norris, C., & Raab, C. (2006) A report on the surveillance society, Surveillance Studies Network, UK.
Zuboff, S (2019) The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power, Profile Books Ltd.
Helm & Seubert (2020) Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies, Surveillance & Society, 18(2).