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 poor*. 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.

© 2023 Respective authors. This is an Open Access work licensed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public licence (CC BY-NC-ND 4.0). To view a copy of the licence, visit https://creativecommons.org/licenses/by-nc-nd/4.0/