# Online Surveillance in a Swedish Context

## *Between acceptance and resistance*

Coppélie Cocq,[I] Stefan Gelfgren,[II] Lars Samuelsson,[II] & Jesper Enbom[III]

[I] Department of Cultures, University of Helsinki, Finland & Humlab, Umeå University, Sweden
[II] Department of Historical Philosophical and Religious Studies, Umeå University, Sweden
[III] Department of Culture and Media Studies, Umeå University, Sweden

**Abstract**

Users of digital media leave traces that corporations and authorities can harvest, systematise, and analyse; on the societal level, an overall result is the emergence of a surveillance culture. In this study, we examine how people handle the dilemma of leaving digital footprints: what they say they do to protect their privacy and what could legitimise the collection and storing of their data. Through a survey of almost 1,000 students at Umeå University in Sweden, we find that most respondents know that their data are used and choose to adjust their own behaviour rather than adopting technical solutions. In order to understand contemporary forms of surveillance, we call for a humanistic approach – an approach where hermeneutic and qualitative methods are central.

**Keywords**: online surveillance, surveillance culture, soft surveillance, privacy paradox, digital humanities

## Introduction

"We collect information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products, such as people you communicate with the most or groups you are part of. […] We use the information we have (including your activity off our Products, such as the websites you visit and ads you see) to help advertisers and other partners" (Facebook, 2020).

"When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content" (Google, 2020).

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

Above is a brief overview of what we agree to when we use Facebook and Google (other services have similar terms of agreements). Some people might think these terms of agreements are just and fair – others regard them as a severe and intrusive form of surveillance. "[Surveillance] is something that everyday citizens comply with – willingly and wittingly, or not – negotiate, resist, engage with, and, in novel ways, even initiate and desire", to quote David Lyon (2017: 825).

From this vantage point, our aim is to study the paradoxical relationship between how we, on the one hand, negotiate and resist what is seen as unjust or intrusive surveillance yet, on the other hand, willingly and wittingly surrender our personal data through, for example, our use of social media, our shopping habits, smartphones, and credit cards – information that is often open and free to use for compiling datasets to map, analyse, and interpret our lives (compare to the privacy paradox, which we will return to later; see Barth & de Jong, 2017; Norberg et al., 2007). Today, the large amount of digital information provides previously unseen opportunities to harvest data, linking different datasets together, thereby obtaining new information about our lives and behaviours. This is done by both public and private actors. The question is, how do "ordinary" people act and think in such a situation – through acceptance, resistance, or something in between?

The issue of surveillance has been relevant for decades, articulated, for example, in George Orwell's classic dystopian novel *Nineteen Eighty-Four*, written in 1949. In recent years, in the wake of, for example, 9/11 in 2001, the Snowden revelations in 2013, and more recently the American election of 2016 and the Cambridge Analytica scandal of 2018 (Cadwalladr & Graham-Harrison, 2018), it is clear that the forms of surveillance have shifted and that they are affecting our everyday lives.

In order to understand contemporary forms of surveillance in general, and how people live and act under such conditions in particular, we propose a humanistic approach to the issue – using a hermeneutic and qualitative method that acknowledges the complex nature of humankind. This is in line with what David Lyon calls upon to study "the culture of surveillance" (2018), or "surveillance culture" (2017). In this regard, we must acknowledge the currently messy and all-intrusive nature of surveillance, as well as the complex nature of people trying to navigate this culture. Here, we focus on the latter: the people. Where Lyon (2017: 837) states that "the concept of surveillance culture should be developed to understand more clearly the relations between contemporary surveillance culture and the everyday lives of those who might be described as subjects", we aim to highlight and interpret how people (consciously or unconsciously) navigate the (or their) world of data.

This article focuses on young adults in Sweden in their role as people being surveilled (although they are also surveillers, e.g., on social media), and their attitudes and practices towards data harvesting and analysis. How do they relate to the fact that their data are collected, analysed, and distributed through the different services they use online? What measures and strategies do they use to protect their data? What would make them accept these services, data harvesting, and analysis? How can the users' online behaviour be understood in relation to the so-called privacy paradox discussed in surveillance studies research?

## Method

This article focuses on a group of students at Umeå University, Sweden, and comprises approximately 1,000 responses to a questionnaire about online practices and attitudes to surveillance. The group is not representative of the Swedish population as a whole, given that its members are students (some of them former students) who are relatively well educated, as all of them are attending university or have completed university-level education. They are also familiar with computers, using the Internet, and social media communication – and to some extent are aware of the pitfalls and potentials of digital communication.

Even though the students comprise a specific subset of the population, we regard this group as particularly relevant to this study. Of the Swedish adult population, 41 per cent received a tertiary education in 2016, which ranks Sweden 13th in the OECD countries (Swedish Higher Education Authority, 2018). For the participants in this sample, being online is an essential requirement: all of them have been assigned to a web-based learning platform. To a large extent, they also communicate and engage in online activities outside study contexts. As one respondent stated, "I'm forced to use Facebook if I want a social life". We also assume that their educational background suggests that their approach to the pros and cons of digital communication is relatively well informed. In terms of the tendencies and correlations between the variables in which we are interested, this group suits our purposes and can be seen as an illustrative case.

However, we want to emphasise that we have not treated our results according to strict statistical methods. At this stage, our purpose is to identify patterns and highlight dilemmas, potential outcomes, and ways of handling these dilemmas in relation to the overall theme of surveillance.

In a Swedish context, surveillance has primarily been studied from a legal or state perspective. Our focus on Internet users' practices of, experience of, and attitudes to surveillance provides new insights into the perception of surveillance and strategies of acceptance, negotiations, and resistance.

## Surveillance: What it meant during the analogue era and what it means today

Surveillance has traditionally been broadly defined as "focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction" (Lyon, 2007: 14). Surveillance and the registration of people's opinions, values, and actions is a sensitive and often-discussed topic – in Sweden as well as globally.

Surveillance was originally associated with totalitarianism, in line with Orwell's *Nineteen Eighty-Four* (1949) and Foucault's *Discipline and Punish* (1979), in which "the few" are monitoring "the many" in a panopticon-like situation. For a long time, the debate and the research on surveillance was focused on how government agencies surveil ordinary citizens and the dilemmas that could arise from such surveillance, as well as the extent to which surveillance is to be considered an integral aspect of modern society (going back to Foucault, for example). Among these dilemmas is the trade-off between keeping the nation safe and the respect for fundamental rights of privacy (e.g., Flyghed, 1992; Gunnartz, 2006). For example, Thomas Mathiesen (1997) complemented

the panopticon perspective with the synopticon perspective, emphasising how, in the late twentieth century, "the many" turned their gaze to "the few", stressing the role of mass media. In the years to come, the rise of surveillance practices in the wake of 9/11, the increasing distribution of mobile devices, and the proliferation of social media around 2010, along with the associated companies, have blurred the lines between the surveiller and the surveilled. For example, Doyle (2011) criticised Mathiesen for omitting (or ignoring) the impact of Internet technology. Nevertheless, identifiable actors, such as the state, military, specific companies, and so forth, were engaged in surveillance – in other words, a surveillance society (see also Lyon 2001).

In an attempt to categorise the different forms and purposes of surveillance, Marx (2006), Kerr and colleagues (2006), and Nagenborg (2014), for example, used "soft surveillance" as opposed to "hard surveillance". According to Marx (2006), soft surveillance is spreading rapidly outside the traditional boundaries of government and police enforcement. Its consequences are often hidden to those of us who voluntarily contribute to the flow of information.

In studies from the following years it becomes clear that such a distinction between hard and soft surveillance is difficult to maintain, and that the flow of technology, methods, and data between public authorities, the military, and private companies has put us in a situation in which surveillance has become intertwined with our lives (e.g., Ball & Murakami Wood, 2013). The authorities keep track of us (e.g., Barnard-Wills, 2012; McCahill & Finn, 2014), but companies also thrive on our data, trying to predict and steer our behaviours and consumer patterns (Ball, 2017; Zuboff, 2019), all growing organically and without apparent agency (e.g., Haggerty & Ericson, 2000). And in all of this, as ordinary users, we contribute with our data as monitored citizens through healthcare, schooling, and banking systems; through using infrastructure for heating, electricity, and communication; through accepting membership cards and customer surveys; and (not least) through using social media, shopping online, and using services for our mobile devices to function (Ball, 2017; Haggerty & Ericson, 2000; Zuboff, 2019). Thus, preemptive policing and marketing go hand in hand.

In this situation, people have to navigate – accept, resist, or find ways of negotiating costs and benefits (if possible at all, but that is another question). We cannot avoid (some of) our data being collected. Haggerty and Ericson (2000) call this our "data double", which follows us from the cradle to the grave, since it is intertwined with modern society and its welfare systems, and we cannot avoid it as part of our increasingly digital lives (Zuboff, 2019). Choices made by users have proven to be complex and contextual (Trepte et al., 2020). In order to understand the considerations made by individuals about online self-disclosure, aspects such as social context – and, some would argue, the affordances of the technologies (Culnan & Armstrong, 1999; Laufer & Wolfe, 1977; Trepte et al., 2020) – must be taken into account.

According to what Smith (2018) describes as "data doxa", the fabric of data and the surveillance culture restricts our ability and willingness to criticise these conditions. This is because, since our birth, we are entangled with data and 1) believe in data analysis for our security, 2) cannot envision a life (in a welfare state) without data collection, and 3) since our increasingly digital life, on and through digital services, we regard data collection (i.e., surveillance) as normal. Smith is rather pessimistic about people's ability to make conscious and informed choices:

> It is more an effect of fear, habit ignorance and seduction, where an increasing familiarity with the dependence on data obscures a capacity to perceive, let alone question, their broader history and probable trajectory from a critical perspective. (Smith, 2018: 12)

While Smith talks about "data doxa" as key, Lyon (less pessimistically) talks about a surveillance culture in which "its key feature is that people actively participate in an attempt to regulate their own surveillance and surveillance of others" (2017: 824). Out of fear, familiarity, and pleasure, people can respond to surveillance or take initiatives to become surveillers, although, according to Lyon (2017: 836), the outcome is related to both personal and contextual factors, and he calls for a "careful, critical, and cultural analysis of surveillance situations". People are complex and live in a situation in which privacy is neglected, calculated, or negotiated. Perhaps they are uninformed and unable to critically assess all the parameters (in line with Smith), or perhaps they at least try to do their best to become involved in, or counteract, surveillance (in line with Lyon). This is what we intend to study in this article.

Previous research has analysed attitudes to surveillance in relation to issues of trust. Institutional trust and social trust (interpersonal trust) have been identified as being correlated to people's acceptance or suspicion of surveillance. A number of studies have proved the role of social and institutional trust in the acceptance of surveillance. For example, Denemark (2012) has shown a correlation between institutional trust and acceptance of counter-terrorism policing (see also Friedewald et al., 2015; Strauss, 2015). Additionally, level of education (Budak et al., 2015; Patil et al., 2014; Watson & Wright, 2013) and age (Patil et al., 2014) are factors to which attitudes to surveillance appear to be related. Svenonius and Björklund (2018) also argue that sensitivity to privacy and existential concerns are additional aspects to be taken into account, as they also explain attitudes to surveillance and issues of trust. In a Nordic context, Sønderskov and Dinesen (2016) "find strong evidence of institutional trust influencing social trust", based on datasets from Denmark.

According to the The Swedish Internet Foundation's latest report about Swedes and the Internet (Internetstiftelsen, 2019), 98 per cent of households have Internet access and 95 per cent of the population stated that they use the Internet. The report also reveals a "growing concern that public authorities in Sweden – and large companies such as Google and Facebook – will infringe on our personal privacy online" (Svenskarna och internet, n.d.: para. 4) and that nearly one half of Swedes feel they are being monitored online. However, the report declares that "only one fifth are concerned by the Swedish authorities infringing" (Svenskarna och internet, n.d.: para. 14).

The Nordic countries are said to be "remarkable with respect to high levels of both social trust and, to a lesser extent, institutional trust" (Delhey & Newton, 2005; Sønderskov & Dinesen, 2014; Zmerli et al., 2007; cited in Sønderskov & Dinesen, 2016: 187), referring to data from the World Values Survey (WVS) and the European Values Survey (EVS). Considering the large number of Internet users and the high percentage of Internet accessibility, and in relation to Sweden being a "high-trust country" (see, e.g., Delhey & Newton, 2005), according to research based on data from the WVS and EVS, we find that Sweden is a particularly interesting country for investigating attitudes to surveillance.

## Survey data

Our data comprise 958 responses to the questionnaire. As previously mentioned, these individuals are either students or former students from a broad range of courses and programmes (teacher training, philosophy, informatics, engineering, etc.) on campus and online, indicating that we have a geographical distribution. The overall gender distribution is about equal, even though it differs across different courses and programmes. Of the respondents, 57 per cent are current students and 60 per cent are young adults between 20 and 29 years of age (2% are students below the age of 20).

The survey is aligned with previous studies in other European contexts (see, e.g., Svenonius & Björklund, 2018; Sønderskov & Dinesen, 2016). For background, we inquired about the level of trust in fellow citizens (social trust) and societal institutions and authorities (institutional trust), including the media (e.g., both public service and so-called alternative media), the parliament, the police, as well as researchers. We also inquired about the kind of societal issues that might cause the respondents to feel anxiety in the near future (e.g., terrorism, climate change, xenophobia, or unemployment). Our intention here was to create a general picture of trust and anxiety in order to correlate it with the correspondents' use of, and views about, digital media and data usage.

Furthermore, we asked about the online services that the respondents use, such as Facebook, Instagram, Snapchat, and so forth. The intention was to gain an overview of media channel usage and to get a sense of the specificity of the respondents' Internet usage. For example, we felt confident that Facebook and Instagram would be among the most widely used services, but we also asked about other popular services such as Twitter, Discord, WhatsApp, and Reddit. We wanted to establish whether there was a correlation between more advanced use of digital media and an awareness of issues related to data usage and integrity. By "advanced use", we mean use that goes beyond, for example, consuming online content and online banking and shopping – that is, being part of online communities and production of online content (see also Bruns, 2008).

We also asked about the extent to which the respondents used specific services or practices in order to protect their privacy. Did they use encrypted communication services or a VPN tunnel to hide their online identity? Did they browse in private mode and avoid certain services in order to protect their data? Did they put a piece of tape over their web camera, or simply avoid sharing private information? The different kinds of practices say something about data awareness and about the measures taken to protect personal integrity.

Did the respondents feel uncomfortable because their data can be used by many different actors? Does it make a difference if their data are used by state authorities, companies or organisations, or just by other people? Or is there a concern that the respondents cannot express themselves, be their authentic selves online, or tend to end up in a filter bubble in which information is "gatekept" to suit their own preferences?

Finally, we asked whether it was possible to accept data collection, coordination, and analysis based on what the data was being used for. Is it possible to legitimise data usage if it leads, for example, to better online services for the individual, if you have the option to consent to the use of your data, or if data can be used for the benefit of society at large (for health-related reasons or in order to improve crime prevention)?

## Results

Overall, we found a relatively high level of trust (6–10 on a scale of 0–10) in societal institutions and public services, with the exception of the parliament and politicians. For example, 89 per cent of the respondents rated their level of trust from 6–10 for researchers, 84 per cent did so for the police, 80 per cent for the Swedish Tax Agency, and 77 per cent for the healthcare authorities, while 47 per cent of the respondents had a high level of trust in the government and only 30 per cent in politicians. In this respect, our respondents tended to confirm what has been observed in other datasets in which Swedes have comparatively high trust in societal institutions and the authorities (in line with the results from the EVS). There is a rather low level of trust in alternative media compared to mainstream media and public services: 11 per cent of the respondents rated their level of trust from alternative media from 6–10 and 24 per cent did so for the popular press/tabloids, while 70 per cent rated their level of trust for daily newspapers from 6–10 and 80 per cent did so for public service. Of societal issues that may cause anxiety, xenophobia (69%) and climate change (78%) were greater concerns than war (24%), terrorism (34%), and surveillance (41%), although this naturally varied in the group of respondents (September–November 2019, pre-Corona). Regarding the online services used, most respondents use well-known digital media and services such as Facebook (58%), Messenger (63%), Instagram (57%), YouTube (44%), and Snapchat (38%) on a daily basis and, to a much lesser extent, services such as Twitter (9%) or Reddit (8%).

Regarding counter practices, the respondents appeared to self-censor by not sharing private material more so than by making active use of specific services for encryption and anonymisation, with the exception of browsing in private mode and disabling location services. Some respondents stated how they avoided sharing private material (76%), avoided using services because of the way they gather data (53%), or disabled position services (59%). Around one half of the respondents (45%) used private mode when surfing, and one third (37%) covered their web camera. Only a small minority used encrypted communication (8%), VPN (23%), or search services that do not log their data (10%) in order to protect their data integrity.

The respondents tended to think it was important to be able to remain private online, but there were variations in attitudes: some thought they had nothing to hide – or simply thought that they had to share their data in order to use a service that everyone else was using; and some considered that taking countermeasures was too complicated. In addition, some appeared to not know how to protect their data. On a 0–10 scale, 10 being the highest answer, 60 per cent of the respondents marked one of the alternatives 6–10 for the claim that it was important to be private or anonymous online; 40 per cent did so for the claim that they had nothing to hide and therefore did not care; 31 per cent thought that caring was too complicated; and 36 per cent said that they were well aware of how their data was being used online.

We also asked the respondents about whether there were any circumstances that would make collecting, sharing, and storing their online data more acceptable to them. A general tendency is that people are unwilling to negotiate about their private data in order to get better services (24% for response alternatives 6–10) or customised ads (14% for alternatives 6–10) – in fact, the primary reason why service providers track our data. The main reason why some respondents accepted data gathering and analysis on a larger scale is because they are given an option to consent to how their data will

be used (52% if alternatives 6–10 are included, 63% if alternative 5 is included), and if their data could be used for the greater good of society (55% if alternatives 6–10 are included, 69% if alternative 5 is included). In other words, people want to be in control of their data; they want to know what is happening with their data and how their data are being used. However, for the greater good of society, the majority of respondents were willing to contribute their data (which could be related to the level of trust in official authorities in Sweden).

Surveillance and data usage apparently engaged respondents, even though the level of applying practices for protecting data and personal integrity was rather low. Some easily accessible counter practices were used (self-censorship, private mode, and taping over or disabling a web camera); however, it was less common to install and use software and services to protect a person's integrity. It is obvious that there are several topics that require further investigation in order to gain in-depth knowledge about attitudes towards online surveillance. Below, we examine and discuss our results in relation to the users' negotiations of privacy.

## The privacy paradox in practice: Acceptance, resistance, and negotiation

Overall, our results confirm the seemingly paradoxical pattern that can be recognised in previous studies and which is usually referred to as the privacy paradox, that is, the "discrepancy between individuals' intentions to protect their own privacy and how they behave in the marketplace" (Norberg et al., 2007: 101; see also, e.g., Kokolakis, 2017 for an overview). More specifically, we discerned the following tendencies among our respondents:

1. They value their privacy and integrity online.
2. They are aware that their data might be collected and eventually shared.
3. They consider this collection and sharing of their data difficult to justify on the part of the service providers.
4. They try to handle this situation by adjusting their behaviour rather than through technical solutions.
5. They willingly and wittingly give away certain personal information, for example, by sharing pictures on social media platforms such as Facebook and Instagram.

These results align well with the privacy paradox. However, while they may appear paradoxical, they can be interpreted in ways that do not ascribe systematic contradictory behaviour to people.[1] We believe that one important and largely overlooked key to such an interpretation may lie in the results regarding the respondents' views on what might justify online surveillance (in the sense of making it more acceptable to them). Let us look more closely at the tendencies we have identified.

The results of the survey indicate that the majority of users value their privacy and integrity online and are aware that their data might be collected and eventually shared. However, the results do not indicate that services and strategies for protecting privacy and data are commonly used (e.g., Gerber et al., 2018), as illustrated in Table 1.

***Table 1.*** *Practices and strategies for protecting privacy (per cent)*

| Service or strategy | Yes | No | No answer |
|---|---|---|---|
| VPN | 23 | 77 | 0 |
| A browser that does not save your inquiries (DuckDuckGo, etc.) | 10 | 89 | 1 |
| Private/secret mode in your web browser | 45 | 54 | 1 |
| Disabled location services | 58 | 41 | 1 |
| Encrypted communication (e.g., Tor, Signal) | 7 | 92 | 1 |
| Cover your computer camera | 37 | 62 | 1 |
| Avoid certain services because of how they collect data about you as a user | 53 | 47 | 0 |
| Avoid sharing private material | 76 | 23 | 1 |
| Other | 2 | 26 | 72 |

*Comments:* The following question was posed: "Do you knowingly use any of the following services or strategies in order to protect your identity and/or information associated with you?" [Yes/No/No response]. The number of respondents was 954.

Of the respondents, 77 per cent stated that they did not use a VPN service, 89 per cent did not use browsers that did not save information or avoided tracking, and 92 per cent did not use encrypted communication. In other words, a large majority of our respondents used a web browser on a regular basis that collected data and did not protect their IP address.

Practices and strategies that were more common among our respondents included disabling location services (58%), avoiding certain services that collected data (53%), and not sharing private material (76%). Other strategies described by the respondents included disabling Wi-Fi when not online, using a fictitious username, and not sharing biometric data like fingerprints.[2]

The survey data indicates that practices for limiting or avoiding the sharing of private data mainly comprised strategies such as considerations regarding where and what to share, rather than making use of technological tools and specific services. For the statement "caring about how data are collected is too complicated", 48 per cent of the respondents disagreed. This indicates that for a large number of users in our sample, their reason for searching for and identifying strategies in Internet behaviour, rather than in technological solutions, was not because of the perceived complexity of caring about how the data was collected.

In other words, the protective behaviours adopted by most of respondents were not "specific computer-based actions" (see also Milne et al., 2009) but were rather what we call avoidance behaviours. These results can be interpreted as an indication that technical solutions – such as VPN and less well-known web browsers – add to the difficulty of understanding what is happening behind the screen (e.g., in relation to algorithms). This may be one explanation as to why most users in our survey opted for avoidance behaviours rather than technological filters when they wanted to protect their privacy. Avoidance behaviours such as not sharing, self-censorship, and so on, imply that the user takes control (or experiences control) of the information. Technological solutions,

on the other hand, require a level of confidence and technical competence. In line with previous research on the topic, we interpret these results in terms of the "perceived efficacy" (Boerman et al., 2018; Rogers, 1975) – in our case, the choices made by most the respondents indicated a low level of confidence in their ability to protect themselves or to be effective when they used technological tools and solutions for data privacy.[3]

The results may also suggest that our respondents – although they value their privacy and integrity online – are not unduly worried about the potential harm they may experience personally as a result of their data being harvested by online service providers. They appear to be equally concerned about protecting their data from other people, or, rather, being in control of what data they share and how and where they share it.[4] A consideration in favour of such an interpretation is that most of our respondents actually reported that they willingly and wittingly gave away some of their personal information. Most of the respondents (81%) stated that they sometimes shared pictures on social media. This is in line with Facebook (91%) and Instagram (81%) being among the platforms that were most used by the respondents, of which the majority reported daily use (58% and 57%, respectively). Sharing pictures is an important part of these platforms, particularly Instagram. At the same time, 76 per cent of the respondents in our study claimed that they avoided sharing personal data online.

Sharing material on social media has been an important aspect of the rise in self-branding, sometimes referred to as "personal branding" (Khamis et al., 2017). In the context of online surveillance, the proliferation of self-branding raises a number of questions. Does it contribute to enhancing acceptance among everyday social media users – like the respondents in this survey – to giving away their personal data online? After all, four out of five of our respondents claimed to share pictures online. In contrast, does the growth of self-branding make individuals more aware of what kind of information they are sharing? From this perspective, the claim by 76 per cent of the respondents that they avoided sharing certain private data could be seen as a conscious act of self-branding – a form of strategic sharing. In any case, our results indicate that sharing some personal information (such as pictures) is important to most of our respondents and sometimes overcomes their concerns about disclosing their personal information.

Other survey results indicate that these concerns may be at least partially ethical or ideological, rather than solely based on self-interest (a discussion largely absent in surveillance studies, according to Lyon, 2017). In discussions of the privacy paradox, it is typically assumed that people try to act rationally in order to further their own self-interest (e.g., Barth & de Jong, 2017; Gerber et al., 2018). According to one of the most-established descriptions of the privacy paradox, often referred to as the "privacy calculus" (Lee & Cook, 2014 Gerber et al., 2018), "a user is expected to trade the benefits that could be earned by data disclosure off against the costs that could arise from revealing his/her data" (Gerber et al., 2018: 229). However, it is not only self-interested concerns that may make people opposed to being surveilled online. We asked the respondents about the extent to which certain conditions would increase their acceptance of their personal data being stored and shared when they are online; the answers are presented in Table 2.

These results suggest that it is difficult to gain people's acceptance of being subjected to online surveillance. Even if the conditions mentioned in Table 2 were met, this did not generally increase the respondents' acceptance of having their information collected

***Table 2.*** *Acceptance of personal data being stored and shared (per cent)*

| Condition | 0–4 | 5 | 6–10 | No opinion/ No answer | Most frequent response |
|---|---|---|---|---|---|
| That it is required so that others can develop and give you access to desirable services. | 49 | 16 | 24 | 11 | 0 (18%) |
| That you receive personal, customised offers and search results (based on your previous online activities). | 69 | 12 | 14 | 5 | 0 (30%) |
| That it facilitates some of your online activities (access to various services, online shopping, etc.). | 51 | 15 | 29 | 5 | 0 (17%) |
| That you are able to consent to your data being stored and shared when you choose to use a certain service. | 33 | 11 | 52 | 4 | 10 (14%) |
| That society can benefit from the data about you that is being stored (e.g., to combat criminality/ terrorism or achieve health benefits). | 24 | 15 | 55 | 6 | 5 (15%) |

*Comments*: The following question was posed: "To what extent would the following conditions increase your acceptance of your personal data being stored and shared when you are online?" [where 0 represents "not at all" and 10 represents "100%"]. For each condition, the table shows the percentage of respondents who marked, respectively, some of the response alternatives 0–4, response alternative 5, or some of the response alternatives 6–10 (or who reported having no opinion or chose not respond). It also shows the response alternative that was most frequently used for each condition and what percentage of the respondents that number represents. The number of respondents was 954.

and shared. Not surprisingly, with respect to increasing the respondents' acceptance of such data being stored and shared, the conditions that scored highest were that they had given their consent to it and that society could benefit from it. Nevertheless, for both of these conditions, quite a high number of respondents (33% and 24%, respectively, for alternatives 0–4) did not think that they made the sharing and storing of their personal data more acceptable.

Yet, as we noted above, most of our respondents reported that they used well-known digital services such as Facebook and Google on a daily basis, with 79 per cent stating they used Facebook a few times a week at a minimum. This may be taken to indicate that although the respondents find online surveillance hard to justify, they do not consider such surveillance first and foremost to be a threat to their own self-interest. It may simply be that they find it morally objectionable that service providers surveil people's activities online (unless they have clearly received their consent).

If it is a correct interpretation that people often object to online surveillance on ethical or ideological grounds, rather than based solely on self-interest, the five tendencies identified above would seem less paradoxical. People can judge (in line with, e.g., the privacy calculus) that the benefits, in terms of self-interest, of participating on social media and sharing certain personal information, for example, in the form of photos, would probably outweigh the costs. But they can still consistently consider their privacy and integrity to be important issues and regard the surveillance policies of social media providers unjustified on ethical or ideological grounds. As noted above, the measures

taken by our respondents to protect their privacy (i.e., avoidance behaviours) appear to be primarily directed towards other people, aimed at avoiding the wrong people getting hold of their sensitive or private information (by disabling position services and covering the web camera, for example). Willingly and wittingly choosing to share certain information and pictures on social media platforms may not seem risky to people in this respect, but they may still have other reasons for objecting to the collection and sharing of their data.

In other words, acknowledging the full complexity of how human beings navigate the surveillance culture (to borrow Lyon's phrase), incorporating ethical aspects and people's often conflicting interests – for example, sharing information and photos among friends on the one hand, and protecting their privacy on the other – may shed new light on the privacy paradox and help gain a better understanding of people's online behaviour.

## Conclusions

The question of the relationship between surveillance and the attitudes towards it is indeed complex, and therefore warrants further attention. To summarise, we noted two general tendencies in our study:

1. People are aware that their data are used to monitor, analyse, and predict their behaviour, which has advantages and disadvantages on both an individual and a societal level.

2. People try to handle this insight to the best of their ability, using quite down-to-earth and non-technical countermeasures – adjusting their behaviour rather than using, for example, encryption and VPN.

Thus, the question of attitudes toward surveillance is not an easy or straightforward one, particularly not in contemporary society – if we accept the concept of an all-encompassing "surveillance culture" (Lyon, 2017, 2018). The survey demonstrated how people regard data management as being both crucial and difficult to handle at the same time, although the results do not indicate that people surrender to apathy, neglect, or "data doxa" (Smith, 2018). There are many aspects to take into consideration in a society that is increasingly permeated by digital media and data collection and analysis, undertaken by corporations and authorities alike. There are many pros and cons associated with current developments, on both a societal and an individual level. Some people see an Orwellian dystopia à la *Nineteen Eighty-Four* looming large in a near future, in which state authorities and multinational companies are Big Brother. Others (still) see the opportunity to democratically connect and reach other people through digital media, or create and develop a personal brand. And others see the opportunity to solve problems – for example, health, terrorist, and climate-related issues – through the analysis of large amounts of data.

On the one hand, we see how people adapt their behaviour in the knowledge that they are being subjected to surveillance. People avoid using digital media in certain ways or avoid certain services: they put a piece of tape over their web camera, they do not share content considered to be too private, or they disable location services. In other words, they adopt avoidance behaviour – rather than use VPN, encrypted communication, or

other technical solutions – in order to have a sense of control over their data.

On the other hand, we see how people appear to see no alternative to using the digital services that are available to them. If a large proportion of the population (i.e., friends, acquaintances, organisations, and businesses) use a specific service – for example, Facebook – people tend to use that service in fear of missing out on the community and information. Or, if companies provide easy-to-use and accurate services – for example, Google – people appear to think it is acceptable to trade their data in return for the benefits of using the services provided.

An additional aspect relates to how data are used and how usage is restricted by different actors. People are more likely to approve of the use of their data if they are able to consent to such use or if the use of their data is for the common good. Academic research on health and climate change, for example, appears to be considered quite reasonable, whereas market analysis and advertising by commercial actors, or state-imposed intelligence based on the very same data, are frowned upon. Users' – at first sight paradoxical – way of handling privacy and data harvesting can indeed be partially interpreted and explained in terms of ethical and ideological considerations.

Throughout history, people have been known to not be fully rational in relation to the unknown, not least in relation to novel technologies (e.g., Bauer, 1997; Brosnan, 2002), and the current realm of data usage is an unknown and complex territory for many – a territory we all try to navigate from our different understandings. In order to understand the ethics of data usage – or humans and human behaviour in general – in relation to data usage by different actors, not only do we need to take into account and acknowledge the complexity of the contemporary surveillance culture, we also need to take into account people's experiences, attitudes, and interpretations of the same surveillance culture.

**Funding**

This article is part of a project (iAccept: Soft Surveillance – Between Acceptance and Resistance) funded by the Marcus and Amalia Wallenberg Foundation (MAW 2016.0092).

**Notes**

1. Numerous explanations of the privacy paradox have been proposed in the literature (for an overview, see Gerber et al., 2018; Barth & DeJong, 2017) but they typically do not take into account the fact that people's behaviour and attitudes may sometimes be partially explained by ethical or ideological considerations
2. In the survey, the respondents had the opportunity to provide responses other than those suggested in a list.
3. This aspect and the complexity of choices behind avoidance behaviours will be further investigated in our project through qualitative data (interviews).
4. Approximately 41 per cent (alternative 6–10 on a scale of 0–10) of the respondents were concerned about other people getting hold of their data and 52 per cent were concerned about companies and other organisations getting hold of their data. 52 per cent of them were afraid that their data could be used against them.

## References


Ball, K. S., & Murakami Wood, D. (2013). Editorial: Political economies of surveillance. *Surveillance and Society*, *11*(1/2), 1–3. https://doi.org/10.24908/ss.v11i1/2.4933

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

Barnard-Wills, D. (2012). *Surveillance and identity: Discourse, subjectivity and the state*. Farnham, UK: Ashgate Publishing.

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

Bauer, M. (1997). *Resistance to new technology: Nuclear power, information technology and biotechnology*. Cambridge: Cambridge University Press.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 1–25. Online first. https://doi.org/10.1177%2F0093650218800915

Brosnan, M. J. (2002). *Technophobia: The psychological impact of information technology*. New York: Routledge. https://doi.org/10.4324/9780203436707

Bruns, A. (2008). *Blogs, Wikipedia, second life, and beyond: From production to produsage*. New York: Peter Lang.

Budak, J., Rajh, E., & Anić, I.-D. (2015). Privacy concern in western Balkan countries: Developing a typology of citizens. *Journal of Balkan and Near Eastern Studies*, *17*(1), 29–48. https://doi.org/10.1080/19448953.2014.990278

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Delhey, J., & Newton, K. (2005). Predicting cross-national levels of social trust: Global pattern or Nordic exceptionalism? *European Sociological Review*, *21*(4), 311–327. https://doi.org/10.1093/esr/jci022

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

Doyle, A. (2011). Revisiting the synopticon: Reconsidering Mathiesen's 'The Viewer Society' in the age of web 2.0. *Theoretical Criminology*, *15*(3), 283–299. https://doi.org/10.1177/1362480610396645

Facebook. (2020, August 21). Data policy. Retrieved December 7, 2020, from https://www.facebook.com/about/privacy

Flyghed, J. (1992). *Rättsstat i kris: Spioneri och sabotage i Sverige under andra världskriget* [*The constitutional state in danger: Spies and sabotage in Sweden during World War II*]. Stockholm: Federativ.

Foucault, M. (1979). *Discipline and punish: The birth of the prison*. Harmondsworth, England: Penguin.

Friedewald, M., Rung, S., van Lieshout, M., Ooms, M., & Ypma, J. (2015). Report on statistical analysis of the PRISMS survey [Deliverable 10.1, PRISMS Project]. Karlsruhe, Germany: Fraunhofer Institute for Systems and Innovation Research ISI. http://publica.fraunhofer.de/documents/N-367427.html

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

Google Privacy & Terms. (2020, March 31). *Google terms of service.* https://policies.google.com/terms?hl=en-US

Gunnartz, K. (2006). *Välkommen till övervakningssamhället* [*Welcome to the surveillance society*]. Stockholm: Bokförlaget DN.

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *The British Journal of Sociology*, *51*(4), 605–622. https://doi.org/10.1080/00071310020015280

Internetstiftelsen [The Swedish Internet Foundation]. (2019). *Svenskarna och internet 2019* [*The Swedes and the Internet 2019*]. https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2019/

Kerr, I. R., Barrigar, J., Burkell, J., & Black, K. (2006). Soft surveillance: Hard consent. *Personally Yours*, *6*, 1–14. https://ssrn.com/abstract=915407

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

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

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42. https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-4560.1977.tb01880.x

Lee, A., & Cook, P. S. (2014). The conditions of exposure and immediacy: Internet surveillance and Generation Y. *Journal of Sociology*, *51*(3), 674–688. https://doi.org/10.1177%2F1440783314522870

Lyon, D. (2001). *Surveillance society: Monitoring everyday life*. Buckingham, UK: Open University Press

Lyon, D. (2007). *Surveillance studies: An overview*. Cambridge: Polity Press.

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

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

Marx, G. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information – "Hey buddy can you spare a DNA?*"* In T. Monahan (Ed.), *Surveillance & security: Technological politics and power in everyday life* (pp. 37–56)*.* New York: Routledge. https://doi.org/10.4324/9780203957257

Mathiesen, T. (1997). The viewer society: Michel Foucault's 'panopticon' revisited. *Theoretical Criminology*, *1*(2), 215–234. https://doi.org/10.1177%2F1362480697001002003

McCahill, M., & Finn, R. L. (2014). *Surveillance, capital and resistance: Theorizing the surveillance subject*. London: Routledge. https://doi.org/10.4324/9780203069974

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-6606.2009.01148.x

Nagenborg, M. (2014). Surveillance and persuasion. *Ethics and Information Technology*, *16*(1), 43–49. https://doi.org/10.1007/s10676-014-9339-4

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Orwell, G. (1949). *Nineteen eighty-four: A novel*. London: Secker & Warburg.

Patil, S., Patruni, B., Lu, H., Dunkerley, F., Fox, J., Potoglou, D., & Robinson, N. (2014). Public perception of security and privacy: Results of the comprehensive analysis of PACT's pan-European survey [PACT Deliverable 4.2]. Brussels: RAND Europe. https://www.rand.org/pubs/research_reports/RR704.html

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Smith, G. J. (2018). Data doxa: The affective consequences of data practices. *Big Data & Society*, *5*(1), 1–15. https://doi.org/10.1177%2F2053951717751551

Strauss, S. (2015). *SurPRISE synthesis report: Citizen summits on privacy, security and surveillance*. Vienna: Institut für Technikfolgen – Abschätzung / Österreichische Akademie der Wissenschaften. http://surprise-project.eu/wp-content/uploads/2015/02/SurPRISE-D6.10-Synthesis-report.pdf

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

Swedish Higher Education Authority. (2018). *Higher education in Sweden 2018 status report* [Report 2018:10]. https://english.uka.se/download/18.7f89790216483fb85588e86/1534509947612/Report-2018-06-26-higher-education-in-Sweden-2018.pdf

Svenskarna och internet [Swedes and the Internet]. (n.d.). *Summary in English: Meaningful time online and the pros and cons of digital society.* https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2019/the-swedes-and-the-internet-2019-summary/

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

Trepte, S., Scharkow, M., & Dienlin, T. (2020). The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, *104*, 106115. https://doi.org/10.1016/j.chb.2019.08.022

Watson, H., & Wright, D. (Eds.). (2013). Report on existing surveys [Deliverable 7.1, PRISMS Project]. Karlsruhe, Germany: Fraunhofer Institute for Systems and Innovation Research ISI. http://publica.fraunhofer.de/eprints/urn_nbn_de_0011-n-5022795.pdf

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