CHAPTER 6

# Accepting or rejecting online surveillance

## *The case of Swedish students*

LARS SAMUELSSON

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

ABSTRACT

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

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

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

## Introduction

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

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

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

three categories used in this chapter thus capture the main considerations typically referred to in discussions about the justification of online surveillance.

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

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

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

## Theoretical points of departure

The ongoing digital transformation of society has resulted in what David Lyon (2018: 30) refers to as a "culture of surveillance": "the everyday webs of social relations, including shared assumptions and behaviours, existing among all actors and agencies associated with surveillance". In contrast to traditional top-down surveillance, where a state or other entity with authority

constitutes the surveilling agent – Bentham's (1995) Panopticon providing a powerful illustration – surveillance is nowadays to a large extent a more horizontal, sometimes even reciprocal, affair, where many citizens possess the means to surveil each other. In addition, large companies and various organisations have much to gain from collecting information about people, for instance, to use consumer and social media data for marketing purposes (Ball, 2017; Colaresi, 2020; Zuboff, 2019). This situation has been referred to in terms such as new surveillance (Marx, 1998), soft surveillance (Marx, 2005), surveillance capitalism (Zuboff, 2019), and surveillance culture (Lyon, 2014, 2017) – a common denominator being the perception that such surveillance is something that we live in, that surrounds us, and that we need to relate to in one way or another. This comparatively new situation highlights the ethical issue of under what conditions or circumstances surveillance may be deemed acceptable.

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

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

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

largely a question of whether it is beneficial to society (assuming that it is also beneficial to the people constituting the society).

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

## Method and research procedure

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

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

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

able to compare our results with other similar studies using the same scale (see Svenonius & Björklund, 2018).

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

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

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

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

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

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

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

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

## Survey results

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

### *Background data*

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

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

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

### *Acceptance of online surveillance*

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

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

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

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

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

### *Correlations between consent responses and societal benefits responses*

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

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

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

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

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

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

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

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

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

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

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

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

At the same time, however, a noteworthy number of respondents demonstrate an opposite pattern: 24 per cent of the respondents in the

modest acceptance increase interval for the consent condition are in the strong acceptance increase interval for the societal benefits condition (see Table 6.2); 21 per cent of the respondents in the modest acceptance increase interval for the societal benefits condition are in the strong acceptance increase interval for the consent condition (see Table 6.3); 9 per cent of the respondents in the strong acceptance increase interval for the consent condition are in the modest acceptance increase interval for the societal benefits condition (see Table 6.2); and 16 per cent of the respondents in the strong acceptance increase interval for the societal benefits condition are in the modest acceptance increase interval for the consent condition (see Table 6.3). The filtering of results reveals that of the total number of respondents (956), 65 (7%) are found in the strong acceptance increase interval for the societal benefits condition *and* the modest acceptance increase interval for the consent condition, while 39 respondents (4%) are found in the modest acceptance increase interval for the societal benefits condition *and* the strong acceptance increase interval for the consent condition.

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

## Discussion

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

### *Personal benefits*

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

motivation for using such services is arguably for the most part precisely that one hopes to receive some kind of personal benefit. How should we understand these results?

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

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

### *Consent and societal benefits*

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

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

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

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

### *Differences in ethical thinking*

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

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

the consent condition, but not under the societal benefits condition, display a typical deontological outlook (which is compatible with embracing other kinds of ethical thinking as well).

### *Some problematising remarks*

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

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

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

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

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

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

## Conclusion

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

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

## Acknowledgements

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

## References


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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Endnotes

[1] Consider, for instance, the vast literature on the so-called privacy paradox (three comprehensive critical literature reviews are Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017). Illustrative overviews concerning people's online behaviours and attitudes to online surveillance can be found by Auxier and colleagues (2019), Boerman and colleagues (2021), and Madden and Rainie (2015). For studies in a Swedish context, see, for instance, Cocq and colleagues (2020) and Leckner (2018). The present study is not concerned with the different reasons people may have for disliking being surveilled, but with the question of whether there are considerations that could increase their acceptance of online surveillance.

[2] In relation to modern surveillance studies, self-interest has, for instance, been invoked in proposed explanations of the privacy paradox. Several popular explanations of why people seem to behave online as if their privacy were not important to them, while at the same time reporting that their privacy *is* important to them, appeal to a self-interested cost-benefit analysis (Barth & de Jong, 2017; Gerber et al., 2018; Kokolakis, 2017).

[3] It is standard, when introducing ethical theories, to include a third kind of theory, namely, virtue ethics. However, virtue ethical theories are not straightforwardly theories about what makes actions right or wrong, but primarily theories about what characterises a virtuous agent (and the question about which actions are right is then a question about what a fully virtuous agent would do). So, this kind of theory does not fit neatly with the discussion about what considerations may make surveillance acceptable (or right). It may be noted, though, that the discussion about deontological versus consequentialist features has a place in virtue ethics as well, as a discussion about the characteristics of the virtuous agent – to what extent such an agent displays consequentialist and deontological thinking, respectively.

[4] Some versions of consequentialism consider outcomes indirectly: Instead of assessing the value of the outcome of an action directly, they assess the value of the outcome of applying or internalising principles, rules, dispositions, or the like, that recommend or result in the action. In the context of online surveillance, a consequentialist may consider either the consequences of a particular instance of surveillance directly, or, for instance, the consequences of a certain surveillance practice (of an actor). This difference is not important to my discussion in this chapter.

[5] There is, of course, a risk that those who voluntarily choose to participate in a questionnaire survey generally share some characteristics that may affect the responses. In relation to this worry, it is important to (again) note that I do not claim to say anything about other people than precisely those who answered the questionnaire. However, it could also be noted that there is already a selection made regarding which group the survey addresses: young students with considerable digital experience, who spend a large part of their time online. We can expect there to be a general interest among this group in the kind of questions addressed in our survey, and thus, quite a large interest to participate irrespective of one's particular views on the different questions asked. One student group of 90 persons (a subgroup of the total group of respondents) was invited to answer the survey directly in the classroom at the end of a lecture. The teacher left the students and there was no way for the teacher to check if any particular student answered. In this group, the response rate turned out to be close to 100 per cent. Interestingly, the response patterns in this subgroup are generally very similar (for the questions tracking the respondents' attitudes, behaviours, beliefs, views, or opinions) to those in the total group.