TECHNO Review | Vol. 10, No. 1, 2021
International Technology Science and Society Review / Revista Internacional de Tecnología Ciencia y Sociedad
https://doi.org/10.37467/gka-revtechno.v10.2871

EXPLORING THE CULTURE OF SURVEILLANCE:

A Qualitative Study in Portugal

DÉLCIO FAUSTINO [1], MARIA JOÃO SIMÕES [2]

[1] University of Beira Interior, Portugal
[2] University of Beira Interior. Researcher at Interdisciplinary Centre of Social Sciences (CICS.NOVA.UMinho) and LabCom, Portugal

KEY WORDS

Surveillance
Culture of Surveillance
Social Perceptions
Surveillance Practices
Surveillance Awareness
Resisting Surveillance

ABSTRACT

By following the theoretical framework of the surveillance culture this article aims to detail the surveillance imaginaries and practices that individuals have, capturing differences and social inequalities among respondents. We present an in-depth look into surveillance awareness, exploring subjective meanings and the varying awareness regarding commercial, governmental, and lateral surveillance. Furthermore, a detailed analysis is made on how individuals sometimes welcome surveillance, expanding on the cost-benefit trade-off, and detailing it on three distinct trade-offs: the privacy vs. commercial gains/rewards, the privacy vs. convenience and, the privacy vs. security. Lastly, we present a section that explores and analyzes resistance to surveillance.

Received: 09/ 03 / 2021
Accepted: 27/ 03 / 2021

GLOBAL KNOWLEDGE ACADEMICS

1. Introduction

Electronic surveillance can be understood as any personal data collection process that is electronic, systematic, routinized, and concentrated for a given purpose (Lyon, 2014). It is not something particularly new, but in recent years much has changed. As Edward Snowden recently revealed to the general public, nowadays electronic surveillance is no longer exclusively aimed at suspicious targets, it covers almost every citizen.

In a context where the amount of user-generated-data are enormous, access to that data is increasingly important to different entities. The US National Security Agency (NSA) being able to access data provided by several multinational companies such as Facebook and Google, shocked and further alerted the world about electronic surveillance. However, individuals can no longer be seen exclusively as passive agents in the surveillance context.

Today we get involved with surveillance through various ways, for instance, we engage voluntarily in surveillance practices by self-tracking (Ball, Di Domenico, & Nunan, 2016; Charitsis, 2019; Crawford, Lingel, & Karppi, 2015; Lupton, 2014; Lyon, 2018), by using social media platforms where we are simultaneously watching (surveilling) our peers' activities (Andrejevic, 2004, 2005; Lyon, 2018; Marwick, 2012; Marwick & Boyd, 2010) or even to surveil more powerful entities through practices usually associated with *sousveillance* (Ganascia, 2010; Mann & Ferenbok, 2013; Mann, Nolan, & Wellman, 2003). Additionally, for almost every buy we make today we are most likely involved in commercial surveillance, be it through the simple tracking of loyalty cards, online accounts, or even just by allowing cookies to be stored in our devices. Moreover, while we engage in all these previously mentioned practices, all of them are potentially being harvested by governmental agencies to verify if there is something suspicious going on.

We argue that it is crucial to understand that, today, surveillance is not simply something that is "done" upon us. Instead, we are very much involved with it, and one could even argue that it has become a way of being and seeing the world that became symbiotically entrenched in our lives. This new context leaves us with many important questions such as:

- How do individuals perceive electronic surveillance?
- Are they aware of its existence?
- Is surveillance regarded as a positive or a negative thing?
- In what situations are individuals willing to give (or not) their personal data?
- To what extent are individuals resisting surveillance?

Drawing upon Lyon's *Culture of Surveillance* (2018) approach, this article aims to shed light on these questions through two different goals: to explore perceptions that citizens have related to surveillance and to dive into individuals' surveillance practices. This piece is structured into five sections; the first one introduces a brief discussion of the surveillance culture approach and addresses why it is pertinent today. The second section is where we begin presenting the results from the interviews, starting with surveillance awareness. The third and fourth sections are more focused on surveillance practices and detail the willingness to provide (or not) personal data specified into several trade-offs. Lastly, the final section presents the results regarding the resistance to surveillance.

2. A Brief Review of the Surveillance Models of Analysis

Numerous models of analysis have been suggested in surveillance studies. Of special note is Foucault's (1995) panopticon metaphor, the author based his model of analysis on Bentham's design of a prison that was intentionally built to enable all inmates to be surveilled by a single guard. The architectural ingenuity of the panopticon enforced a context where prisoners could never be certain if they were under surveillance or not; consequently, they behaved in a more disciplined and compliant manner. The panopticon metaphor captures the dimensions of self-restraint and self-discipline that an individual might experience when dealing with surveillance. Indeed, Foucault's concept of self-restraint resonates with more recent concepts such as the surveillance chilling effect (Stoycheff, Liu, Xu, & Wibowo, 2018; Widener, 2016). Surveillance chilling is a term commonly used to describe changes in behaviors made by individuals when they are aware of being surveilled to conform with the perceived expectations of the surveillant agents (Manokha, 2018). This author advocates for the value that the panopticon still holds today especially in the organizational surveillance domain. The theoretical richness of the panopticon remains consensual, but several scholars have repeatedly called for surveillance studies to move beyond it, since, among other aspects, it does not capture the active involvement most of us have with surveillance today (Haggerty, 2006; Lyon, 2018). That assertion is especially confirmed when considering the various types of surveillance and the different power relations that they encompass between the surveillant and the surveilled.

Another model of analysis for surveillance is the surveillance assemblage proposed in Haggerty and Ericson (2000), this model is often seen as a successor to the panopticon model (Zaia, 2019). The surveillance assemblage model emphasizes that surveillance is constituted by a panoply of heterogeneous objects whose growth resembles a rhizomatic expansion. Haggerty and Ericson (2000) point out the similarities, in terms of the expansive and regenerative capabilities, that surveillance shares with rhizome. For instance, prohibiting a certain technology will not dismantle the assemblage. Another key contribution of this model of analysis is that, unlike the panopticon model, it captures both the increasing interconnectivity and the changing hierarchies of surveillance.

Finally, despite all the theoretical contributes of the models mentioned above, Lyon (2018), more recently, asserts that we need to approach surveillance differently. Arguing that analyzing surveillance as culture is very enriching for surveillance studies researchers. One of the main characteristics that the *Surveillance Culture* approach conveys is a theoretical framework that helps us grasp the active role of surveillance subjects on surveillance. The surveillance culture approach is a more adequate model to analyze the several ways that individuals participate and contribute to surveillance since its focus is how surveillance is present in everyday life. Lyon suggests two key-concepts to operationalize the surveillance culture – surveillance imaginaries and surveillance practices.

According to Lyon (2018), surveillance imaginaries are basically how surveillance is perceived by individuals or groups of individuals. This concept can include several questions, such as: (i) What is surveillance? (ii) How does it work and who are the surveillant agents? (iii) What are the main goals of surveillance? (iv) Is it good or bad? and many other complex assumptions. Collective assumptions are also imaginaries, such as the growing awareness of electronic surveillance and the belief that data are needed to solve problems. But how are surveillance imaginaries constructed? they are formed through our daily involvement and experience dealing with surveillance. Other external sources such as news and popular media (mainly movies/series, music, and books) are also important when forming one's surveillance imaginaries (Lyon, 2018). Surveillance imaginaries often offer the capacity to act, engage, and legitimate (or not) surveillance practices.

Surveillance practices are basically every action we perform that is somehow related to surveillance (Lyon, 2018). Any behavioral change in response to surveillance is also regarded as a surveillance practice. For instance, users' activity on social media being greatly influenced by their acquaintances using the same platform (Marwick, 2012; Marwick & Boyd, 2010) is a surveillance practice. Other surveillance practices include the previously mentioned self-tracking behaviors or adopting "surveillance neutralization techniques" (Marx, 2016, p. 145), the latter involving actions that seek to resist surveillance. They include both simpler moves, such as covering one's webcam, or more complex ones, such as the installation of privacy-enhancing software, like VPN's.

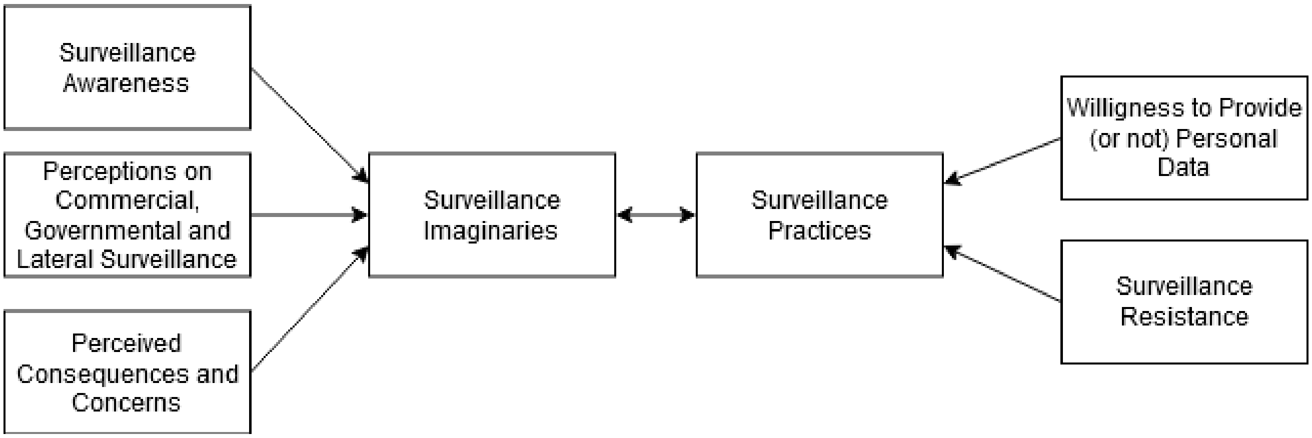
The surveillance practices and imaginaries concepts influence each other mutually (Lyon, 2018). The heterogeneity and immensity of both surveillance practices and imaginaries are arguably impossible to capture in their entirety – since fundamentally they capture everything we think and act upon associated with surveillance.

Many researchers have mapped and explored surveillance practices and imaginaries through other theoretical approaches (Augusto & Simões, 2017; Dinev, Massimo, Hart, Christian, & Vincenzo, 2006; Jansson, 2012; Pavone & Degli Esposti, 2010; Steinfeld, 2017; Turow, Feldman, & Meltzer, 2005; Zurawski, 2011).

3. Method and Procedure

This research was based on a qualitative methodology, and the chosen technique was the semi-structured interviews. In a world where the debate on personal data collection and storage is stronger than ever, we argue that the personal opinions of "regular" citizens about surveillance are important to hear, how do they perceive it, and how do they act towards it. The interview protocol was designed to explore both the interviewee's surveillance imaginaries and practices within the target audience of this study. A thematic analysis of the interviews was performed based on the model of analysis presented in Figure 1.

Figure 1. Model of Analysis


Surveillance Awareness
Perceptions on Commercial, Governmental and Lateral Surveillance
Perceived Consequences and Concerns
Surveillance Imaginaries
Surveillance Practices
Willigness to Provide (or not) Personal Data
Surveillance Resistance

Source: Authors' own figure.

The chosen sampling strategy was stratified and purposeful. According to Schreier (2018), this method is ideal when the researcher wants to explore known or potential factors that might influence the phenomenon under investigation. The chosen factors were age, gender, education level, and general knowledge of information and communications technology (ICT). A total of 16 interviews were conducted in Portugal with individuals who possessed heterogeneous profiles regarding the prementioned 4 factors. Out of the 16 interviewees, 8 were male, and the other 8 females, their age ranged from 22 to 57 and their education level varied from the Portuguese 10th grade to PhD. To capture heterogeneous levels of ICT knowledge, the sampling was made to include both IT experts chosen due to their formal training, and people with different but more limited IT knowledge, and without any formal IT training.

4. Surveillance Awareness and the Different Knowledge About the Three Types of Surveillance

Nowadays, after the Snowden leaks and frequent privacy-related scandals, most citizens are aware of the worldwide use of mass surveillance (Lyon, 2018). Most interviewees in this study were aware, to some extent, of electronic surveillance, although that level of awareness varies a lot between participants. The responses we received from the interviewees indicated that a sort of general knowledge or the reflection on certain aspects of internet navigation seem to significantly contribute to their surveillance awareness, such as personalized ads or recent e-privacy scandals. ICT knowledge and education level seem to be the most important sociodemographic variables when it comes to surveillance awareness, while gender and age take on a secondary role.

When questioned about their thoughts on the general purposes of mass surveillance, most responders showed a greater sensitivity towards commercial surveillance, associating its purposes to marketing goals that seek to maximize profits. Only one interviewee mentioned governmental surveillance. Multiple interviewees showed much lesser knowledge about governmental surveillance when compared to other forms of surveillance. In particular, to some less aware of governmental surveillance, the name of Edward Snowden needed to be invoked to stimulate the conversation. Perhaps this unawareness or unfamiliarity could be partially explained by the sociocultural Portuguese context that our interviewees experienced, which is far removed from the nation's fascist past. Additionally, Portuguese civil society organizations, media, and political parties appear to have been oblivious to the threats to civil and political rights that mass surveillance poses. The surveillance debate in Portugal only took place during the recent COVID-19 pandemic, which occurred several months after the interviews were done.

Of special note was the acceptance by some interviewees and even the appreciation of the existence of governmental mass surveillance because of its potential to aid in fighting crime and improving security. One participant asserted:

> Because I don't have bad intentions, but that's good. For those who have bad intentions, it's good to monitor them because with so much terrorism around, maybe it's a good thing to prevent many things. (E2, female, 40 years old, 12th grade, office worker, Azores).

Among the discourses about governmental surveillance, the "nothing to hide" argument was directly used by an interviewee. This argument has been found in previous surveillance qualitative research (Augusto & Simões, 2017; Solove, 2011). Other interviewees associated governmental surveillance with the privacy vs. security trade-off, which, as Chandler (2009) asserted, is often biased in favor of security. A more detailed analysis on this trade-off is presented later in this article.

All the participants are aware of lateral surveillance especially on social media, but they do not associate lateral surveillance directly with electronic surveillance. This occurs because lateral surveillance does not involve significant power asymmetries, unlike commercial and governmental surveillance. The results point to the way that surveillance has become entrenched in the everyday lives of individuals. As Lyon (2018) claimed, surveillance is becoming a way of watching and being in the world. The participants of this study reported several practices that emphasize this perspective. For instance, the participants engaged in social media to expose the best version of themselves, while simultaneously watching others, and some carefully choosing specific content they wanted to share. Other practices that highlighted the way surveillance is part of the routine of some of the participants was the use of multiple apps or services that fit into the category of self-tracking software.

Commercial surveillance was the type of surveillance more prevalent in our responder's minds. In many cases, commercial surveillance could be associated with the frequent contact by subjects with personalized ads and suggestions that they quickly identified as resulting from the collection and analysis of their data. For example, the following account is illustrative:

> (...) A practical example is when we visit some sites on the internet, some... clothing or travel, or whatever, in the meantime they start to appear later, sometimes we don't even notice how, advertisements on our mobile phone, or another... in some other way even (...).(I8, female, 50 years old, master's degree, graduate staff, Covilhã).

However, a few interviewees do not comprehend the general purposes and interests involved in mass surveillance, seeming to confuse digital surveillance with cybercrime activities such as phishing:

> In that case of... banks or something like that, it can be to find out my passwords or gaining access to my account. (I1, female, 35 years old, 12th grade, operational assistant, Azores).

> Exactly, stealing data. For instance, through PayPal, stealing the bank account data. (I2, female, 40 years old, 12th grade, office worker, Azores).

Of note are the similarities that these responders have on the social demographic level, they do not have a higher-level education nor have worked in more qualified jobs. Throughout the interviews, the researchers discerned that the respondents' knowledge about digital surveillance was slightly diminished. Perhaps, one reason why some citizens with little knowledge of digital surveillance confused it with cybercrime is the strong association between surveillance and police activity in the fight against crime. However, in future research we would like to explore further details behind the rationale for this confusion.

Other interviewees mentioned mass manipulation as one of the main aims of surveillance. A young medical student (I7) mentioned the Facebook-Cambridge Analytica data scandal to make his point, saying that we already witnessed an attempt to influence individuals' votes during the American 2016 Presidential Election. A university assistant professor (I16), promptly pointed out that the aim of such publicity was to create needs that "ultimately, in a more dystopian logic, mean controlling people (...)." These reflections on surveillance suggested a more informed and in-depth reflection, which may be closely linked to higher levels of surveillance awareness.

Regarding surveillance-related concerns, a significant number of responders promptly pointed out their privacy concerns, but for several of them, these worries were perceived as a minor concern. This was especially noticeable in interviewees possessing a vast knowledge of electronic surveillance and its mechanisms, these respondents seemed to be indifferent to the consequences of electronic surveillance and even tried to take advantage of it. Such approaches were exemplified by the statements as:

> (...) it's no longer a surprise for me that it's happening, simply if I see it I'm like... ok it's cheaper here, let me see, (...) if it's a product that I really want, it's something that is actually helping me searching what I want faster (I12, 25 years old, bachelor's degree, master's student on IT engineering, Santarém).

Perhaps I12's approach resulted from a rational approach where the surveillance subject believed he could take advantage of the positive aspects of surveillance, while avoiding the negative ones. This approach echoes the results from a study done by Turow et al. (2005), where more informed individuals took a similar approach.

Alternatively, responders who had very little knowledge about digital surveillance were very worried about it, especially those who confused cybercrime with digital surveillance, since they perceive it as a direct threat to their online accounts. According to Lyon (2018), these perceptions may result from a lack of knowledge on how data are collected and analyzed, which can lead to individuals not being aware of even the most basic characteristics of mass surveillance.

Lastly, two interviewees reflected on the link between a strong concern about surveillance and paranoia. Authors such as Giroux (2015), Holm (2009) and Lyon (2019) have also mentioned this link. Holm (2009) noted that when one adopts several behaviors as a response to mass surveillance, one might be easily deemed as having a pathological and unjustified phobia. Two interviewees seemed to entertain the same line of thought:

> Look, not on the basis of what I already told you, I'm not very paranoid, (...) perhaps, I am a bit careful with cameras. (I3, male, 35 years old, 12th grade + technical course (IV) in IT, taxi driver, Azores).

> (...) They [regarding people that are significantly worried about surveillance] are probably paranoic or have something to hide. (I4, male, 25 years old, 10th grade, waiter, Azores).

5. Willingness to Provide (or not) Personal Data

Several interviewees exclaimed that they only gave away their data in situations where it was mandatory to access a certain service/product. This approach often leads to cases of a semi-forced acceptance, which can point to different kinds of surveillance practices, such as providing fake personal data, avoiding websites/platforms that have mandatory personal data requests, and in some cases, the respondents just accept giving away their personal data reluctantly. The following testimonies accurately described most of the responders' practices associated with this theme:

> Look, I give them reluctantly (…). First, I even avoided certain services, but now I think that I created a tolerance effect that is not good (…), I don't feel comfortable. (E16, female, 42 years old, PhD, Assistant Professor, Viseu).

> (…) Usually, I don't give them. So, there is not the factor of me giving them in certain some aspects and not giving them in other aspects, on the internet I do not give them. And when they suddenly ask me for them, I usually lie, I do not insert the real data. (I9, male, 57 years old, 12th grade, operational assistant, Covilhã).

In contrast, interviewee 7 adopted a different and more unconcerned approach by arguing that he always gives his personal data because he is not a "person of interest."

The context of the data collection request seemed to be crucial for the responders' willingness to give away (or not) their data. Most interviewees preferred giving their personal data to public entities rather than to private ones. In most cases, this approach was easily explained by the perception that public entities were more subject to accountability, and also rated better in their purpose for data collection. While for others it was indifferent if the entity requesting data was public or private. For these respondents, it all depended on the purpose of the data collection request. Kennedy, Elgesem, and Miguel (2015), and Marx (2015) similarly pointed out the adequacy of the requested data significantly influenced the responders' surveillance practices in terms of the purpose for its collection. In certain situations, the interviewees understood that giving their data was mandatory in order to access certain services (e.g., accessing public online services or generating online orders). Consequently, they were more willing to give access to institutions in those situations. However, they are much less comfortable in providing personal data when the respondent did not recognize the usefulness of the private data for the functional requirement of a certain service, application, or platform:

> (…) the smart weight scale app, a guy steps on top of the scale and what's funny about that app is that it makes you turn on the GPS, why? Why does that app need to know where I am at to weigh me? Is it because in different parts of the world I am heavier or lighter? (I3, male, 35 years old, 12th grade + technical course on IT (level IV), cab driver, Azores).

Such inadequate data requests were considered by Gu et al. (2017) as unnecessary privacy invasions and proved to be especially disturbing for several interviewees in this research.

5.1 The Chilling Effect

The chilling effect often leads to self-censoring practices, already identified in common everyday practices, such as using social media (Marwick, 2012; Marwick & Boyd, 2010) or Wikipedia (Penney, 2016). To explore the chilling effect influence on the participants' practices, they were questioned about their feelings on their internet activities, i.e., "were online activities altered in any way due to the awareness of mass surveillance?". The interviewees divided into two groups, those who did alter their activity and those who did not. However, the chilling effect was felt with varying intensities among interviewees. One respondent self-censored personal practices due to the fear of decontextualization or misinterpretation of posts on social media:

> All it takes is a post that I find funny, but that in some way can create some susceptibility to other people, for instance, a joke that involves gender inequality, for instance, there are some jokes that are still funny, but we can't share it because we want to avoid being in a tight spot (I12, male, 25 years old, bachelors, master's student on IT engineering, Santarém).

While others, when considering web searches, mentioned that the only theme where they felt conditioned and acted more carefully when searching terms on Google that could somehow be linked to terrorist activities.

Nonetheless, other interviewees did not feel conditioned at all and just posted and searched, regardless of the search terms:

> No, it is more of my decision. I am the one who wants to post it (…). For instance, when I post something it is a photo of me because I am or was in some location. It is spontaneous (…). (I1, female, 35 years old, 12th grade, operational assistant, Azores).

> Hmm no, when I want to search something, I just do it, I just search for it. (I6, male, 47 years old, 12th grade, business owner, Lisbon).

6. The Several Trade-Offs Revolving Around Surveillance Practices and Imaginaries

Personal data holds an important monetary value for different entities. But how do individuals value their own data? To answer this question, we explored the ways our participants approached several situations where they could opt to indirectly exchange their personal data for certain benefits. Multiple interviewees seemed to approach these situations through a cost-benefit analysis, which could be further detailed in three trade-offs – the privacy vs. commercial gains/rewards trade-off, the privacy vs. convenience trade-off, and, lastly, the privacy vs. security trade-off.

6.1 The Privacy vs. Commercial Gains/Rewards Trade-off

Regarding the privacy vs. commercial gains/rewards trade-off, most individuals are not aware of the specific methods used to collect our personal data. That information is very rarely communicated transparently by the collecting entity. Many organizations are interested in our data for different reasons. Commercial entities are focused on extracting value from personal data through social sorting their clients (Gandy, 1989; Lyon, 2015; Pridmore, 2012). Among other things, this technique allows the entities to reduce costs, to enhance marketing efficacy, and to improve their power of persuasion through the personalization of their offers (Ball et al., 2016; Lyon, 2015; Pridmore, 2012). To persuade clients to provide them with personal data, the entities usually offer some sort of commercial benefit in exchange for the data. Alternatively, the entities might try to frame volunteering personal data as a convenience matter by adding certain impediments to whoever refuses to give their data, such as blocking access to their website or an online application (Wottrich, Reijmersdal, & Smit, 2018; Zurawski, 2011).

Our interviewees' perspectives and actions regarding commercial surveillance seemed to highlight the ambivalence surrounding its positive and negative aspects. All respondents recognized the benefits offered in exchange for their personal data at some point in the interviews, although, they were also worried about its effects on their privacy. There was, however, an exception that might be related to respondent not linking the loyalty cards of familiar companies, such as the Portuguese retail chain *Continente*, to commercial surveillance. Conversely, some interviewees revealed a preoccupation with being potentially manipulated into buying more than they originally desired.

Several interviewees felt reluctant to provide their personal data, but when confronted with several commercial benefits that might result from it, they ended up conceding their data; consequently, engaging in privacy vs. commercial gains/rewards tradeoffs. When questioned about commercial entities' loyalty cards, the interviewees responded:

> Yes, yes, I have them it's almost unavoidable. Due to the discounts and so on (…) it is another way of giving data that we should not. (…) but it is true that we give some data, and yes, I have some (I10, female, 52 years old, PhD, teacher in Highschool, Braga).

> (…) At first I am being offered an advantage, but the disadvantage is that they know my whole life, and I don't know if they should do it, but that's it, they do. Basically, I am part of their database, they know and I and all the other citizens who have a card, all the purchases we make, right? (I6, male, 47 years old, 12th grade, business owner, Lisbon).

Some interviewees addressed situations as a cost-benefit trade-off, where they could opt to furnish personal data in exchange for commercial gains/rewards. Surrendering their data seemed to bring more benefits than costs, most often than not. A similar approach was reported by Zurawski (2011), where the participants were not significantly influenced by their awareness of data collection when accepting to trade their personal data for commercial benefits, even when they showed some concerns regarding their privacy.

Similarly, some interviewees were aware of both positive and negative aspects of commercial surveillance; but ultimately saw it as "fair" or even advantageous for themselves. One interviewee addressed the personal data–commercial benefits trade-off directly and adopted a rational and economical attitude:

> "(…) I'm not that kind of person that goes hey I'm going to get this card, it can save me 1 euro… that I won't do, unless it is something that I use a lot… for instance for every time that I fuel my taxi, I save about 3 euros and 70 cents in a tank. At the end of summer, I get a lot of money for that, that makes it worth" (I3, male, 35 years old, 12th grade + technical course on IT (level IV), taxi driver, Azores).

He seemed to attribute economic value to his personal data, a discount of 1 euro was not enough to convince him to sign up for a loyalty card. But, when considering a more frequent and higher discount, he changed his approach and accepted trading his personal data for more advantageous commercial benefits, an aspect that was already noted in Acquisti, Taylor, and Wagman (2016). Winegar and Sunstein (2019), in a recent quantitative study, explored the value consumers placed on their data privacy in terms of monetary value, and concluded that the median amount a consumer is willing to pay would be $5 per month to maintain data privacy, while demanding about $80 to permit access to personal data. Although it was not possible through the interview to discern what exact value I3 attributed to the access to his personal data, he appeared to have one value in mind and his surveillance practices were significantly influenced by it.

6.2 The Privacy vs. Convenience Trade-off

Today, indirectly exchanging personal data for convenience has become quite common, even if an individual is not aware of its occurrence. Park, Chung, and Shin (2018) argued that the cognitive process required to comprehend the potential costs to one's privacy when using platforms that collected data was too much of a burden. As a result, many individuals focus on the immediate benefits and the convenience that was being offered to them, rather than on the potential privacy costs. Surveillant platforms deliberately explore this vulnerability through the exploitation of the so-called softening of surveillance trend, where surveillance is carried out in a much more subtle and less invasive way (Marx, 2015). The platforms use sophisticated knowledge on human behavior to persuade individuals to concede their data (Acquisti, Brandimarte, & Loewenstein, 2015).

Even those who are more reluctant to concede their personal data will often end up quitting the trade-off exercise when confronted with so many elaborated strategies to persuade the individual to surrender data. Such strategies include a variety of subtle ways, such as presenting pop-ups asking for informed consent that are much easier to accept than to reject; or more direct ones like blocking access to everyone who refuses to allow personal data to be collected. Some interviewees noted, for instance, that the informed consent pop-up text that usually was displayed when visiting a website was generally hard to read and not "transparent". Two participants argued that the informed consent text was intentionally designed to persuade acceptance of data collection:

> I hope they rethink the way in which they inform us of what is being requested and how it is going to be used, which normally… is a set of information that nobody reads, it is impossible to read that until the end, and I think this is intentional. (I16, female, 42 years old, PhD, assistant university professor, Viseu).

> (…) It is written in a very extensive, very complex way and for which people do not have time. For example, when we go to create a web page, something I learned in my degree, is that people are willing, to reach their goal, they are only willing to give three clicks, (…) if a person only wants to give three clicks to reach the goal, why is it that a person who is on that site and wants to be quick to find something, is going to take the trouble to be reading something so extensive, nobody does it (…). (I12, male, 25 years old, degree, master's student, and researcher in computer engineering, Santarém).

These results raised questions about how the informed consent forms are being presented to individuals. The recent directives approved by the European Parliament often imply that websites must ask for informed consent before collecting individuals' data; but as mentioned, commercial entities seem to have bypassed this activity by simply transforming the informed consent pop-up to an inconvenience matter process – making it difficult to fully read and rejecting it a time-consuming and *click demanding* option. In response to these factors, multiple interviewees declared that the pop-up just bothered them, and they just click "accept" as quickly as possible to reduce the nuisance. In fact, data collection of informed consent forms is often so difficult to read or interpret that they can purposefully fail to warn individuals about the data that is collected. Some interviewees do not even realize that their data could be used for commercial motives:

> (…) I think that for example in certain apps, we had to know or be warned that… that they are using our data for their benefit. (I2, female, 12th grade, office worker, Azores)

> (…) That it can be sold? That has never happened to me that they would sell my data, I was never showed a statement like "can we sell your data? (I5, female, 23 years old, bachelor's degree, master's student in political science, Porto).

Apparently, the decision to allow web cookie storage (or not), is unaffected by its content. The interviewees seemed to have previously decided that refusal was the preferable option, even if they did not read the content of the notification. The most important factor in this decision-making process appeared to be the inconvenience that rejecting the notification could imply. As Rogers (2008) noted, when faced with such situations, most individuals accepted the option that came as the default and was more convenient – simply accepting.

6.3 The Privacy vs. Security Trade-off

Most governmental agencies recognized the value of personal data in order to improve security (Hong, 2017) and increase governance quality. These appear to be the two typical arguments to justify implementing new or reinforced surveillance programs. This approach is often closely related to the so-called privacy-security trade-off, which caught the attention of several researchers in the last decades (Augusto & Simões, 2017; Chandler, 2009; Hong, 2017; Pavone & Degli Esposti, 2010; Simões & Jerónimo, 2018; Solove, 2011). According to these studies, it was fairly common for a surveillance subject to think that by sacrificing privacy, the subject would be contributing to improved societal security. Even though the increment of the security obtained through mass surveillance is still far from proven (Hong, 2017; Pavone & Degli Esposti, 2010). In fact, the analysis of the privacy-security trade-off, when considering governmental surveillance, has been identified as inadequate by Pavone and Esposti (2010). The authors argued that privacy and security are not exchangeable goods; hence, they cannot be traded. But despite the debate around the privacy-security trade-off, its presence in individuals' perceptions is not disputable. Several interviewees perfectly approached the trade-off mentioned above:

> I don't mind that they see my personal data, as long as I don't have a bomb at my doorstep, do you know what I mean? Because of the Islamic terrorists (I7, male, 20 years, 12th grade, medicine student, Braga).

That being the case, other multiple interviewees recognized the potential benefits for security that could be achieved by sacrificing some of their privacy. Nonetheless, they questioned the current balance of the privacy-security trade-off.

> (…) through that situation [governmental mass surveillance] it is possible to flag many tax frauds for instance, or even other crimes! But the problem is, how far does the invasion of personal life have to go to enable that? (I14, female, 40 years old, PhD in IT, IT specialist, Covilhã).

Ultimately, it seemed that the participants that considered mass surveillance as fundamental to ensuring safety also appeared more likely to willingly concede personal data to governmental agencies. Moreover, others, (who showed more privacy concerns), questioned governmental surveillance's efficacy and the costs that it could imply to one's privacy.

7. Resisting Surveillance

As more recent literature suggests, in today's context citizens are not simply passive subjects; instead, they can engage in several actions to negotiate surveillance. When contemplating mass surveillance and the chances of being able to resist it, an individual must reflect upon the enormous power asymmetry that resisting organizational surveillance implies. Currently, locating information on how to confront mass surveillance and avoid being monitored is relatively easy. A quick search on Google furnishes several websites that present numerous ways to overcome mass surveillance (Marx, 2016). Nonetheless, even adopting several of these strategies does not facilitate immunity to surveillance. Several entities, such as governmental agencies or major corporations, could overcome these surveillance neutralization techniques. For instance, these institutions delete adulterated data or bypass the anonymization process that some tools provide to users by means of far superior technological resources and technical skills than the average internet user (Howe, 2015). But the question is: To what extent are institutions willing to spend significant resources to bypass strategies? If most individuals use surveillance neutralization techniques, then bypassing them will become much harder and, thus, a much more resource-demanding task (Acquisti et al., 2015) – something that might challenge the profitability or feasibility of data collection. The neutralization techniques listed in Marx (2016, p. 145) captured a wide spectrum of potential actions that aim to resist surveillance. However, they include actions that do not apply to digital surveillance practices. For that reason, some neutralization techniques were not considered for this study, and others were slightly adapted to better capture the participants' practices as outlined in Table 1.

Table 1 – Surveillance Neutralization Techniques

Neutralization Technique	***Action***
Avoiding	Purposely choosing locations or contexts where an individual thinks that surveillance will not be present, (e.g., avoiding accessing certain platforms).
Refusing	Simply refusing to give certain information, (e.g., rejecting requests for the storage of cookies)
Distorting	Altering input such that a technically valid result is detected by the data collection system, but the inference drawn from it is invalid (e.g., giving false information when a platform asks us for our personal data).
Masking	Blocking access to data produced and adding deception factors such as a fake location or IP address, (e.g., using proxies or VPN's).
Breaking	Rendering a surveillance device inoperable, (e.g., covering a webcam with a sticker)

Source: Adapted from Marx 2016:145.

The surveillance neutralization technique that was most often employed by the interviewees was *Refusing*. Most participants preferred refusing to store web cookies on their devices. It is noticeable among those refusing the web cookies pop-ups, some opted for a more decisive refusal and simply search other ways to access the content they wanted to retrieve, while others accepted reluctantly to access contents that they considered especially appealing. Several interviewees admitted that they never fully read the web cookie pop-ups. Only four read the pop-ups, suggesting once more that these notifications for consent were usually filled with subtle strategies that make reading them an unpleasant and time-consuming effort.

Certain participants also engaged in several surveillance practices that could be considered an *Avoiding* technique. The adopted practices were: careful and limited use of GPS and Wi-Fi in their smartphones; selective web navigation; and lastly, one participant asserted that he prefers to use Short Message Service (SMS) since its operation does not require going through the internet.

Only two interviewees referred to practices related to the *Masking* technique, referring the use of proxies and virtual private networks (VPN's). Interestingly, despite the increasing worldwide use of VPN's and proxies (Mardisalu, 2019), the only participants to report the usage of these tools had IT formal training. This situation raised some questions about the social inequality separating those with more knowledge of ICT and surveillance neutralization techniques from those with less.

Conversely, the *Distorting* technique was commonly used by participants with different levels of IT knowledge. The most common practice was furnishing fake personal data. Furthermore, this practice, in some cases, was related to the context where their data was requested:

> For example, … when I order, when I order from a website, from a store, for example, (…) I just put the data, my data, nothing special, (…) it asked for the address to send the order, but this is normal, today this is the norm. (...) Now, for example, sometimes to enter certain games, applications, to play I have already entered data like… I just create a random email and insert any name (…) and then I can just play the game. (I13, male, 24 years old, 12th grade, security guard, Covilhã).

Generally, the responders were willing to provide their actual personal data in situations where the veracity of the data were needed to comply with their request. For instance, in e-commerce an individual's address is crucial so that an order can be delivered to a home or office location. Alternatively, when facing data requests that were not crucial for the functioning of a certain platform or application, multiple interviewees simply provided fake data. These surveillance practices are related to the importance of the purposes and context of the data request, which was also mentioned in other surveillance studies such as Marx (2016) and Kennedy et al. (2015)

Practices related to the Breaking technique were also mentioned by multiple interviewees who declared that they usually cover their webcams. One interviewee also mentioned that he deactivates his computer's microphone. Both of these practices are most likely related to the so-called webcam hijacks and the scandals involving virtual assistants such as Siri or Alexa recording its users without their consent.

8. Final Considerations

Lyon's (2018) theoretical framework on the surveillance culture and the concepts of surveillance imaginaries and practices have proven useful to analyze and explore the rich panoply of heterogeneous perceptions and practices regarding surveillance of our research subjects. Using the surveillance culture approach allowed to capture, in a more comprehensive way, the characteristic that individuals might actually welcome surveillance in certain situations (see the Trade-Offs section) and voluntarily engage in self-tracking practices.

The option of analyzing commercial, governmental, and lateral surveillance as distinct phenomena proved particularly enriching, since respondents espoused different levels of awareness, perceptions, and practices. Among the three types of surveillance that were explored in this study (commercial, governmental, and lateral), commercial surveillance was the most easily identified by all the participants. Participants' own online navigation experiences were, in many cases, responsible for this perception. While responders were aware of lateral surveillance, they did not associate it directly to digital surveillance. Governmental surveillance, on the contrary, was much less referenced and most participants were poorly informed about it. In some interviews, governmental surveillance was seen as something "distant" or as a work of fiction. While most interviewees recognized the need for governmental surveillance and accepted it to a certain extent, their perspective changed significantly when addressing specifically the occurrence of mass governmental surveillance on the web. The opinion of multiple interviewees suggested they perceived this issue to be exaggerated. Further research is necessary to identify whether such responses reveal a lack of knowledge, little awareness of the risk, or attitudes of devaluation or denial.

Most participants recognized the ambivalence surrounding commercial surveillance by relating both its positive and negatives aspects. By exploring the participants' own perceptions and opinions, they appreciated commercial surveillance even when they were aware of the risks of potential privacy invasion that was posed. Consequently, the participants did not appear to willingly offer their personal and private data, but they did accept the need to exchange it in situations where they saw a benefit to surrendering the private or personal data.

Fundamentally, our participants engaged in the full range of three privacy vs. benefits trade-offs. The privacy vs. enhanced security, most visible in governmental surveillance, and two other trade-offs that are most visible in commercial surveillance, the privacy vs. commercial benefits, and the privacy vs. convenience trade-off.

Organizations have been presenting data collection consent notifications to comply with the recent directives implemented in the European Union, this has facilitated the use of the *Refusing* technique by individuals. However, as Marx (2016:168) asserted, surveillance resistance must be analyzed as a "… dynamic adversarial social dance involving strategic moves, countermoves, and counter-countermoves.", *Refusing* can be perceived as a surveillance resistance move by individuals; but organizations countermoved by making the consent notifications recurrent, hard to read, time-consuming, and designed with other subtle mechanisms to persuade the user to accept without reading them. As a result of this countermove, the decision on whether to give or not to give consent for data collection has often turned into a mere *click*, exclusively motivated by convenience; this helps to explain the contradiction between the interviewees' discourse and practices. Even though all the participants declared that the consent notifications for data collection were crucial, most of them did not take the time to read the material because of an organization's countermove. Finally, as long as it is possible (or legal) to prevent individuals from accessing a website or platform by rejecting the consent notifications for data collection, users will always be vulnerable to semi-forced uninformed acceptance.

By analyzing the responders' perceptions and experiences with data collection consent notifications, the manner that such notifications are presented should be seriously considered for alteration. Perhaps more dedicated research regarding consent notifications for data collection is needed to further explore this question, but there are at least four elements that need consideration to protect individuals from an uninformed acceptance:

1. the notification should have a limited number of characters and the vocabulary used in it should also be simpler
2. the font should be clear and easy to read
3. in case of not consenting, the period between the rejection and the reappearance of the consent notification should be longer than the current duration
4. the number of clicks necessary to reject the notification should be equal to those necessary to accept it.

Some inequalities were identified when it came to surveillance awareness and surveillance resistance. These inequalities appeared to be related to the general social inequalities involving the access and use of ICT that remain significant today. While some interviewees knew about the fundamental mechanisms of mass surveillance, others had limited knowledge about these mechanisms and even confused mass surveillance with cybercrime. These inequalities were also visible in the neutralization of surveillance. Some techniques or moves required more knowledge or resources than others. Consequently, individuals with more IT knowledge could, for instance, better utilize some of the most effective neutralization techniques such as masking (e.g., using VPN's and proxies), while others who were unaware of such tools simply resigned themselves to not trying to neutralize surveillance, even though they wished to bring about neutralization. The outcomes of the study suggest that the education level, ICT knowledge, social class, and cultural capital of individuals are variables that play an important role in the inequalities of dealing with surveillance. The study of these variables and their relation to the mentioned inequalities should be deepened in the future through quantitative studies.

Interestingly, the interviews seem to have caused certain reflexivity in the participants regarding surveillance practices. Some interviewees reflected, seeming to undertake some kind of self-assessment, about the possibility of “negotiating” surveillance in a more adequate way. Additionally, several interviewees with lower surveillance awareness manifested their intention of adopting a more careful approach, seeking to make more informed decisions when faced with situations where privacy-related data collection occurs. The results highlight the importance of initiatives that seek to raise electronic surveillance awareness, since the decision of surrendering personal data is at times uninformed.

Lastly, there is a need for recurrent research on surveillance practices and imaginaries, since both are prone to significant changes as new information, contexts and technologies emerge.

Author's note

This article is based on the field work performed within the scope of the master’s dissertation in Sociology: Exclusions and Social Policies entitled “Culture of Surveillance in Portugal: perceptions and practices” by Délcio Faustino, defended in 2020 at University of Beira Interior. The first author appreciated all the guidance provided by Professor Maria João Simões throughout the research and participation on this article.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492. https://doi.org/10.1257/jel.54.2.442

Andrejevic, M. (2004). *Reality TV: The work of being watched*. New York: Rowman & Littlefield.

Andrejevic, M. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society*, *2*(4), 479–497. https://doi.org/10.24908/ss.v2i4.3359

Augusto, F. R., & Simões, M. J. (2017). To see and be seen, to know and be known: Perceptions and prevention strategies on Facebook surveillance. *Social Science Information*, *56*(4), 596–618. https://doi.org/10.1177/0539018417734974

Ball, K., Di Domenico, M. L., & Nunan, D. (2016). Big Data Surveillance and the Body-subject. *Body and Society*, *22*(2), 58–81. https://doi.org/10.1177/1357034X15624973

Chandler, J. (2009). Privacy versus national security clarifying the trade-off. In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (pp. 121–138). New York: Oxford University Press.

Charitsis, V. (2019). Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare. *Surveillance & Society*, *17*(1–2), 139–144. https://doi.org/10.24908/ss.v17i1/2.12942

Crawford, K., Lingel, J., & Karppi, T. (2015). Our metrics, ourselves: A hundred years of self-tracking from the weight scale to the wrist wearable device. *European Journal of Cultural Studies*, *18*(4–5), 479–496. https://doi.org/10.1177/1367549415584857

Dinev, T., Massimo, B., Hart, P., Christian, C., & Vincenzo, R. (2006). Internet users' privacy concerns and beliefs about government surveillance: An exploratory study of differences between Italy and the United States. *Journal of Global Information Management*, *14*(4), 57–93. https://doi.org/https://doi.org/10.4018/jgim.2006100103

Foucault, M. (1995). *Discipline and punish: The birth of the prison*. New York: Vintage Books.

Ganascia, J. (2010). The generalized sousveillance society. *Social Science Information*, *49*(3), 489–507. https://doi.org/10.1177/0539018410371027

Gandy, O. H. (1989). The surveillance society: Information technology and bureaucratic social control. *Journal of Communication*, *39*(3), 61–76. https://doi.org/10.1111/j.1460-2466.1989.tb01040.x

Giroux, H. A. (2015). Totalitarian paranoia in the post-orwellian surveillance state. *Cultural Studies*, *29*(2), 108–140. https://doi.org/10.1080/09502386.2014.917118

Gu, J., Xu, Y. (Calvin), Xu, H., Zhang, C., & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Haggerty, K. D. (2006). Tear down the walls: On demolishing the panopticon. In *Theorizing Surveillance: The panopticon and beyond* (pp. 23–45). Portland: Willan Publishing.

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

Holm, N. (2009). Conspiracy theorizing surveillance: Considering modalities of paranoia and conspiracy in surveillance studies. *Surveillance and Society*, *7*(1), 36–48. https://doi.org/https://doi.org/10.24908/ss.v7i1.3306

Hong, S. H. (2017). Criticising surveillance and surveillance article critique: Why privacy and humanism are necessary but insufficient. *Surveillance and Society*, *15*(2), 187–203. https://doi.org/10.24908/ss.v15i2.5441

Howe, D. C. (2015). Surveillance countermeasures: Expressive privacy via obfuscation. *Datafied Research*, *4*(1), 88–98. https://doi.org/10.7146/aprja.v4i1.116108

Jansson, A. (2012). Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of

Sweden). *European Journal of Communication*, *27*(4), 410–427. https://doi.org/10.1177/0267323112463306

Kennedy, H., Elgesem, D., & Miguel, C. (2015). On fairness: User perspectives on social media data mining. *Convergence*, *23*(3), 270–288. https://doi.org/10.1177/1354856515592507

Lupton, D. (2014). Self-tracking Cultures: Towards a Sociology of Personal Informatics. *Proceedings of the 26th Australian Computer-Human Interaction Conference on Designing Futures: The Future of Design*, 77–86. https://doi.org/10.1145/2686612.2686623

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Lyon, D. (2015). The Snowden stakes: challenges for understanding surveillance today. *Surveillance and Society*, *13*(2), 139–152. https://doi.org/10.24908/ss.v13i2.5363

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

Lyon, D. (2019). Surveillance capitalism, surveillance culture and data politics. In *Data Politics* (pp. 64–77). London: Routledge. https://doi.org/10.4324/9781315167305-4

Mann, S., & Ferenbok, J. (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance and Society*, *11*(1–2), 18–34. https://doi.org/10.24908/ss.v11i1/2.4456

Mann, S., Nolan, J., & Wellman, B. (2003). Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance and Society*, *1*(3), 331–355. https://doi.org/10.24908/ss.v1i3.3344

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance and Society*, *16*(2), 219–237. https://doi.org/10.24908/ss.v16i2.8346

Mardisalu, R. (2019). VPN Statistics and Usage. Retrieved September 15, 2019, from The Best VPN website: https://thebestvpn.com/vpn-usage-statistics

Marwick, A. E. (2012). The public domain: Social surveillance in everyday life. *Surveillance & Society*, *9*(4), 378–393. https://doi.org/10.24908/ss.v9i4.4342

Marwick, A. E., & Boyd, D. (2010). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society*, *13*(1), 114–133. https://doi.org/10.1177/1461444810365313

Marx, G. T. (2015). Surveillance studies. *International Encyclopedia of the Social & Behavioral Sciences*, *23*(2), 733–741. https://doi.org/https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Marx, G. T. (2016). *Windows into the soul: Surveillance and society in an age of high technology*. Chicago: The University of Chicago Press.

Park, Y. J., Chung, J. E., & Shin, D. H. (2018). The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence. *American Behavioral Scientist*, *62*(10), 1319–1337. https://doi.org/10.1177/0002764218787863

Pavone, V., & Degli Esposti, S. (2010). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, *21*(5), 556–572. https://doi.org/10.1177/0963662510376886

Penney, J. (2016). Chilling effects: online surveillance and wikipedia use. *Berkeley Technology Law Journal*, *31*(1), 1–55. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645

Pridmore, J. (2012). Consumer surveillance: Context, perspectives and concerns in the personal information economy. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge Handbook of Surveillance Studies* (pp. 321–329). New York: Routledge.

Rogers, R. (2008). Consumer Technology after Surveillance Theory. In J. Kooijman, P. Pisters, & W. Strauven (Eds.), *Mind the Screen: Media Concepts According to Thomas Elsaesser* (pp. 288–296). Amsterdam: University Press.

Simões, M. J., & Jerónimo, N. (2018). Rear window - transparent citizens versus political participation. In A. R. Saetnan, I. Schneider, & N. Green (Eds.), *The Politics of Big Data: Big Data, Big Brother?* (p. 358). New York.

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

Steinfeld, N. (2017). Track me, track me not: Support and consent to state and private sector surveillance. *Telematics and Informatics*, *34*, 1663–1672. https://doi.org/10.1016/j.tele.2017.07.012

Stoycheff, E., Liu, J., Xu, K., & Wibowo, K. (2018). Privacy and the panopticon: online mass surveillance's deterrence and chilling effects. *New Media and Society*, *21*(3), 602–619. https://doi.org/10.1177/1461444818801317

Turow, J., Feldman, L., & Meltzer, K. (2005). *Open to exploitation: American shoppers online and offline*. Pennsylvania: Annenberg Public Policy Center of the University of Pennsylvania.

Widener, P. (2016). E-fears, e-risks and citizen-intelligence: The impacts of surveillance on resistance and research. *Surveillance and Society*, *14*(2), 277–285. https://doi.org/10.24908/ss.v14i2.6271

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy*, *42*(3), 425–440. https://doi.org/10.1007/s10603-019-09419-y

Wottrich, V. M., Reijmersdal, E. A. Van, & Smit, E. G. (2018). The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, *106*, 44–52. https://doi.org/10.1016/j.dss.2017.12.003

Zaia, M. (2019). Exploring consciousness: The online community's understanding of mobile technology surveillance. *Surveillance and Society*, *17*(3–4), 533–549. https://doi.org/10.24908/ss.v17i3/4.11934

Zurawski, N. (2011). Local practice and global data: Loyalty cards, social practices, and consumer surveillance. *The Sociological Quarterly*, *52*(4), 509–527. https://doi.org/10.1111/j.1533-8525.2011.01217.x