The End of Privacy? Paradoxes and Dilemmas of Internet Use and Online Surveillance

Carolyn Gaumet[1]

ABSTRACT

With the Internet growing in importance in our daily lives, concerns about privacy and data protection have emerged. While people worry about where their data may end up, they continue making themselves openly transparent by sharing information about themselves and their lives online. This study aims to understand the paradoxes between privacy considerations – mainly, the wish to keep individual data private and secure – and the actions that people undertake in reality. More specifically, it focuses on three paradoxes and dilemmas of privacy: age, perceived usefulness, and rewards. These will be studied by analyzing the results of a survey, in which respondents from the EU, North America and East Asia were asked about their online habits and their opinions on various security issues and privacy measures. The analysis ultimately aims to further the understanding of privacy paradoxes, and to find out what hinders people from protecting their data sufficiently.

1. Introduction

The development of the Internet – followed by the boom of social networking sites, smartphones, and apps of all kinds – rapidly and drastically transformed our day-to-day lives. In 1993, two years after the launch of the World Wide Web, there were approximately fourteen million Internet users and 130 websites (Murphy & Roser, 2018). Fifteen years later, over four billion people worldwide are connected (Kemp, 2018). Since its inception, the Internet has continuously become more abundant, more connected, and more global. People now send emails frequently, chat with friends through social media, and post pictures of their lives. We need to be online and connected to perform many activities that have become necessary in today's society. The Internet has infiltrated our lives at all levels, from work to holidays, from dating to transport. People can check reviews before buying a product, can buy anything they need without leaving their home, and can quickly access any type of information through Google. The Internet is convenient, it is quick and it is easy. However, we rarely ask ourselves how much of our personal data is processed in each simple action.

In 2013, Edward Snowden leaked documents stating that the US National Security Agency (NSA) and various other intelligence agencies were checking phone and e-mail records of citizens[2]. This revelation, along with the disclosures from WikiLeaks since 2006, brought new discussions on transparency. Indeed, transparency needs to be addressed alongside privacy and surveillance, the latter of which shows a paradoxical element to transparency. More recently, the Cambridge Analytica and Facebook data scandal brought a new gravity to privacy and data protection issues, as up to 87 million Facebook users may have been affected by this incident (Solon, 2018). On the other side of the world,

[1] Carolyn Gaumet received a bachelor degree in European Studies at Maastricht University in 2018. Contact: c.gaumet@student.maastrichtuniversity.nl

[2] The full series of articles on the leak are available at: https://www.theguardian.com/us-news/the-nsa-files

the news of China's Social Credit Score system created new fears that governments could use citizens' personal information and data to create rankings (Botsman, 2017), which would bring us dangerously towards a society as imagined by the dystopian series Black Mirror (Brooker, 2011).

This timeline has raised individual awareness over privacy predicaments and the uncertainties of surveillance. However, despite people seemingly disapproving of government surveillance, it appears that only very few are concerned or take necessary measures in protecting their privacy. Therefore, this study aims to answer the question: Why do people experience so much difficulty in striking a balance between privacy and surveillance online?

This paper investigates the lack of transparency in surveillance, bringing forward the paradoxes and contradictions hindering a balance between personal privacy and online surveillance. In order to do so, I conducted a survey to measure individuals' use of apps and websites, knowledge of privacy issues, and personal opinions on surveillance. The paper starts by explaining data gathering and defining surveillance and surveillance societies. The subsequent establishes the paradoxes of privacy, which are used as a guideline for the analysis. Following this, the third chapter defines the selected methodology, by explaining the choice of a survey and how the data was collected. This chapter also includes the formulation of the hypotheses guiding the research. The hypotheses are developed in the next chapter, in which the results of the survey are analyzed and discussed, to gain a better understanding of the paradoxical actions of Internet users.

2. Surveillance Societies and Data Gathering

People have long been concerned about the topic of surveillance, as well as the ways in which it affects privacy. As the concept on surveillance guides this paper, understanding what it means is an important first step. Surveillance refers to the "collection and processing of personal data, whether identifiable or not, for the purpose of influencing or managing those whose data have been garnered" (Lyon, 2001, p. 2). It has transformed our ways of seeing as well as our ways of being seen (Gangneux, 2014). The concern over privacy and surveillance has become particularly visible in the aftermath of 9/11 and subsequent terrorist attacks, after which there was a noticeable increase in security and surveillance measures.

Several scholars note that we are quickly turning into a "surveillance society" (Chen, 2008; Levi & Wall, 2004; Lyon, 1994; Norris & Armstrong, 1999), where our day-to-day lives are shaped and influenced by surveillance measures. The pervasiveness of surveillance technology jeopardizes our rights to privacy and our anonymity. In urban spaces, CCTV cameras, as well as GPS devices and digital cameras have become omnipresent. Surveillance blurs the lines between the private and the public, bringing up questions on where to draw those boundaries. The relationship between who is watching and who is watched is one of control and power, where it becomes difficult to determine who is being protected of what and by whom. Surveillance causes uneven power distribution, which can be noticed in the imbalance between personal and mass surveillance (Wall, 2006). Powerful corporations are indeed more capable of undertaking large-scale surveillance schemes than average individuals.

Surveillance involves power, which has expanded in the Internet era. The Internet itself contributed to the rise of a strong and influential electronic surveillance system. Castells (2001) believes that if this system develops further, it will lead to a decrease in liberty, giving individuals "no place to hide" (p. 181). Authors such as Foucault (1995), Turow (2005) and Castells (2001) view surveillance as being overall negative. The Internet is a space out of which many opportunities may arise, but it is also a

technology of control (Castells), which developed due to the interests of both political and economic actors. Institutions and corporations are able to monitor online behavior, by controlling a network and using centralized databases. Surveillance and identification technologies are intertwined, they have the ability to locate the average user, who is imprisoned in "an architecture he or she does not know" (Castells, p. 171).

Additionally, the development of technology and its infiltration into all aspects of our daily lives has made surveillance even more pervasive and invisible. These technologies can include smart floors, toilets, and light switches, which are all essentially unescapable and therefore provide new opportunities for data collection, general observation, and surveillance. Consequently, in most public and semi-public locations, individuals cannot be certain if they are being watched or not. They will therefore generally assume that they might be under surveillance, which means that they will monitor their own behavior and obey a form of authority (Foucault, 1995). Mann, Nolan and Wellman (2003) address the digital divide, that is, the unequal access to surveillance technologies between corporations and institutions, versus the general public. As cameras and microphones have invaded public spaces, privacy in these places has become at best a challenge, at worst an impossibility. It has however been largely accepted by people, due to a lack of options. Recently, cameras with facial recognition have been used to scan crowds, for example during Occupy Wall Street demonstrations, as a way to keep tabs on protesters (Gladovic, 2017). This suggests a certain abuse of power.

Security is however not the only factor responsible for increasing surveillance measures. Money may also determine these measures, for instance through marketing. According to Zurawski (2011), global data flows lay the foundation for practically every digital consumer-monitoring strategy. In an Internet-based global economy, generating, processing, and trading data is crucial. It facilitates advertisement and marketing, making it more likely to obtain a thriving economy. As Turow (2005) explains, online media is interested in gathering data on their users and audiences, with the aim to sell this data to advertisers. Following this, advertisers can use the collected data to establish a more efficient form of marketing. He argues that consumer and online audiences will see surveillance as an acceptable trade-off to access media freely, which is a factor that will be assessed later in this paper.

Finally, mobile phones are perhaps the most aggressive collectors of data. As we use them throughout the day, wherever we go, and to engage in various acts, they facilitate the tracking of individuals and the mapping of behaviors (Gladovic, 2017). It is possible to know exactly who someone is talking to, where they are going, and follow their tracks throughout their day. The ways in which we use our phones, including our use of social media, makes it easier for corporations to profile the users. Furthermore, third parties are now present in most of our navigation. And while we may not know what their surveillance consists of and what their goals are, they have the ability to track the users' personal information. Unfortunately, as Gangneux (2014) explains, there is no credible alternative to this current surveillance society. People may not be able to identify that they have become objects of surveillance, or they just notice the instant benefits of today's technology, and therefore will ignore some of the dangers that may come alongside it. We find ourselves having to interact with surveillance every day, as it is engrained in our culture. We accept it out of convenience, out of conviction, out of fear, out of entertainment, or even out of boredom. Surveillance can originate at different levels – the state,

corporations, institutions, employers, and even individual actors such as spouses and neighbors (Gladovic, 2017). Anyone could potentially be tracking you, from a cell phone company to the government.

3. Privacy and its Paradoxes

The development of smart phones, the appearance of social media, and the dominance of the Internet in people's daily lives have brought forward a need to protect their privacy. Individuals worry increasingly about what happens to their personal data. Data is traded across the world and is critical in terms of consumer-monitoring. Privacy relates to the individual's control over his or her personal information – what information is disclosed, to whom, how, and when. While it would seem unlikely that individuals would simply give away their personal information, as they are becoming more aware of potential risks, most consumer-related data in fact originates from the consumers themselves. This may seem peculiar and to some extent paradoxical. However, it would rather mean that consumers generate this data in specific contexts, while conducting everyday actions (Zurawski, 2011). People, places, and practices therefore make surveillance possible. For Zurawski, surveillance is "a set of places, actions, and narratives about these—often in circumstances where it is not termed or recognized as surveillance at all." (p. 522).

Multiple, multifaceted reasons exist behind the paradoxes of privacy. For instance, since privacy is abstract and difficult to express in specific terms, people struggle to evaluate the potential harms when their privacy is violated. In order to formulate hypotheses to guide the subsequent analysis, this chapter examines more in depth three paradoxes of privacy: the paradox of age, the paradox of usefulness, and the paradox of rewards.

3.1 The Paradox of Age

A prevailing belief suggests that younger people are less concerned with their privacy than older generations are. This impression is closely tied with the boom of social media and social networking sites. The creator of Facebook himself, Mark Zuckerberg, tried to justify the 2010 change in default privacy settings by declaring that "privacy is no longer a social norm" (Johnson, 2010). Blank et al. (2014) consider the new paradox of privacy to be directly tied to the expansions of the site. Indeed, these expansions are now so deeply engrained in their users' social lives that the users feel the need to reveal information about themselves on sites that generally do not provide sufficient privacy and security controls. Through the Facebook change in default privacy settings, back in 2010, everyone using the site was given the possibility to search for anyone's names, gender, city, or any other type of information that might be included. Privacy concerns are constantly increasing, yet at the same time, the belief that younger people are less likely to take control over their personal data and their privacy endures.

In 2006, the privacy paradox surrounding age stated that adults were far more concerned about their privacy being invaded, whereas teenagers, being unaware of the Internet's public nature, give their information away carelessly. Blank et al. (2014) argued that this paradox had greatly changed by 2013. By then, younger people were more likely to take action in protecting their privacy than their parents were, especially on social networking sites. This view is supported by Child and Petronio (2011), who consider that a larger engagement in social networking sites would lead to privacy protection behaviors, for younger generations to a greater extent than older generations. They choose what to share and have become more aware of the risks and benefits of disclosing particular information on themselves.

Furthermore, they are able to navigate more easily from one site to another, from one app to another, in a manner that emanates an ongoing awareness of the use of these different sites.

Younger people may also have a different way of viewing privacy, which creates a generational gap of sorts. Teenagers and young adults appreciate having control over their online lives. As Boyd explains "[k]ids have always cared about privacy, it's just that their notions of privacy look very different than adult notions" (as cited in Johnson, 2009). This thus rejects the idea that younger people are less concerned about privacy. Generations furthermore have different criteria for privacy. To take a more concrete example, given by Child and Petronio (2011), parents can at times upload pictures of their teenage children, which the latter deem mortifying. The teenagers will promptly un-tag themselves from these kinds of pictures, and might make it clear to their parents that this represents to them a breach of privacy. These differences in views among the generations thus add another element to the age paradox.

Previous research has shown mixed results on the age paradox. While Taddicken (2013) found that age and information disclosure did not share a significant association, Blank et al. (2014) found that younger Internet users were more likely to be skilled at increasing their privacy measures. Questions are still present on the ambiguity of age, especially in an online space dominated by social networking sites. There is some remaining uncertainty on the relation between age and privacy, and the ways in which younger Internet users protect their data differently than older people.

3.2 The Usefulness Paradox

This section addresses the dilemma individuals face in terms of usefulness – or, in other words, how people may have become more likely to accept giving their personal data once they feel like this is benefical to them. The Internet is a powerful space of economic surveillance (Elmer, 1997). It uses search engines to map users' behavior online, then uses cookies and other traces to monitor and profile their habits and online consumption. Corporations will furthermore gather demographic information, such as age and gender, in order to target their advertising, hoping to generate more profits.

Marketers are provided with the data that will allow them to determine whether a particular individual could become an "economically viable consumer" (Campbell & Carlson 2002, p. 587). This enhanced form of consumer profiling increases both the effectiveness and the efficiency of the advertisement efforts, thus reducing risks of uncertainty of introducing and selling their goods and/or services. Some people appreciate seeing targeted advertisement on their social media accounts (DAA, n.d.). Indeed, having a personalized online experience carries some benefits. Tailored advertisement keeps websites, blogs and apps free for users, some of which are particularly useful to them. Moreover, these individuals might discover useful products which they might not have found without advertisement tailored to their needs and interests. However, other users get the feeling of being spied on when they see targeted advertisement, and do not appreciate having to trade their privacy for minor utility.

When individuals seek out certain utility instruments, however, they are more likely to be willing to disclose their personal information. Consumers tend to select convenience over protection (Wong, 2017). To illustrate this phenomenon, we can look into various types of online payment. Some examples of this include online banking, booking a flight on a regularly used airline, or frequently shopping on the same online store. In all three of these examples, people may decide to trade elements of their privacy – including here their credit card details and home address, and possibly passport number – for additional

ease and efficiency when making routine transactions. Many people avoid taking actions to preserve their privacy if they will cost them anything, whether time or money (Wong). Therefore, even if they are concerned by the loss of their privacy, their choices might not match their opinions if they are able to gain something useful out of the trade-off.

3.3 The Paradox of Rewards

Being online, and thus being connected to the rest of the world, essentially comes for free. As a free system would not be sustained for long, data becomes a currency. A very valuable currency, particularly for advertisement and marketing purposes. As an example, we can consider an individual who connects onto a health site – perhaps to check some symptoms they have been suffering from. After they have visited the website, their data can be sold to pharmaceutical companies (Gladovic, 2017). While having our data stored and sold in such ways seems disconcerting, many consumers do not worry much about this fact. Some of their data being collected appears to be a fair price, as long as they are able to access information and online content freely.

This feeds directly into the idea of soft surveillance (Marx, 2006), which works with relatively little friction. Consumers actually assist in the generating of data about themselves, with little to no opposition. Additionally, Marx (2006) explains that it is easier for us to cede our personal information when the process of data-collection is "automatic and hassle free and when we are compensated" (p. 40). Moreover, the act of handing over our personal information is ingrained in some of our daily practices, making it harder to avoid. The data we produce as consumers is critical in today's surveillance society. It is used to monitor individuals and track their habits. An example of a daily practice is the use of loyalty cards while shopping. The phenomenon is analyzed in depth by Zurawski (2011), who adds that people are not particularly careful with their information, even when they are aware that it may end up in global flows of data. As the data is generated by the consumers themselves, it is reasonable to expect that it is also produced locally. Hence the data originated in specific places (e.g. supermarkets), within specific contexts of the consumers' everyday lives. Personal data is then used to assess the behavior and consumption patterns of people, in an economy where the establishment of new strategies (such as ones in advertisement) is made dependent on gathering personal information.

Loyalty cards are a part of a category of reward systems. Often, they are delivered to the individual for free, allowing the person to obtain certain bonuses and rewards. This suggests that people are willing to give up their data, as long as they receive something out of the transaction. While this is similar to some points brought up concerning the usefulness dilemma, these dilemmas differ in the sense that the reward is a bonus, something that the individual does not *need* as much as *want*. The reward can also just be a potential for a future gift or even just the promise that the individual will be under consideration for a prize. This dilemma puts forward certain distortions in consumer behavior, especially with regards to privacy (Wong, 2017). A Stanford study conducted to measure the probability of students giving away data, mentioned by Wong, showed that the smallest incentives could influence privacy-related decisions. In this situation, the researchers offered free pizza to a group of students, under the condition that they would disclose the email addresses of three of their friends. Unsurprisingly, the majority of these students picked the pizza rather than the protection of their friends' data. Ultimately, given an appealing incentive, people will very easily surrender their personal information and private data, no matter their opinions of privacy.

4. Methodology

4.1 Formulation of Hypotheses

Based on the research question, this paper's survey aimed to unveil the reasons why people may struggle to find a balance between surveillance and their privacy. Not only did it attempt to reveal the opinions of individuals on privacy measures and data collection, it also aimed to expose the likelihood of individuals giving away their personal data and identify the factors influencing their opinions. The hypotheses were established, built upon the paradoxes presented in the previous chapter:

H1: Age is positively related to the degree of mistrust towards the Internet.

This hypothesis consists of two elements, suggesting that age affects how cautious individuals are towards the Internet. First, the opinions of various age groups on the topic of privacy are compared. The second step focuses on the measures that people of different ages take to protect their personal information. It would seem that younger respondents would be less worried about safety and privacy-related risks than older respondents. Indeed, younger respondents grew up alongside the Internet, possibly making them less likely to be distrustful towards these technologies. Through this hypothesis, the study therefore examines the possible presence of a generational gap. According to Taddicken (2013), self-disclosure behavior is more widespread among younger Internet users, which suggests that they not only use social media and other websites more intensively, but they also are likely to reveal more information about themselves. On the other hand, Blank et al. (2014) believe that the age paradox lies in young people being more likely to actually take action and protect their privacy than their older counterparts. H1 will hence determine if there is an association between age, mistrust towards the Internet and privacy measures, and if so, if it favors the common idea that younger people are careless in terms of online presence and privacy.

In order to measure this hypothesis, six variables are used to compare the degrees of mistrust people may have towards online settings, and six other variables are used to assess the security measures taken by individuals to protect their data. Following this, the age groups were split into two categories to discern the potential importance of a generational gap in terms of online safety.

H2: The perceived usefulness of an app or website is positively related to the likeliness that an individual will give away their personal data.

People seem to consider the trade-off between the usefulness of an app or website and giving away their personal data. This hypothesis therefore suggests that the more useful an app or website is to an individual, the more likely the individual will be to give away his or her personal information. Furthermore, it will not only measure the opinions of the respondents, but will also compare what they say and believe to the actions they undertake. Comparing the perceived usefulness of certain apps to the likeliness that people will disclose their personal information to these apps will help assess the hypothesis. It will also allow to determine whether or not people are coherent in what they believe they do to protect their privacy and what their actual actions show.

H3: Reward systems are negatively related to individual wariness of online risks.

Using rewards and incentives, for example loyalty cards, make users less wary of risks. They will see the benefits and decide that these benefits are worth the cost of giving away their data. This third hypothesis aims to measure whether people are more likely to cede their personal information if they might get a bonus from doing so, as well as the factors that could influence this choice. To measure this third hypothesis, the survey allowed respondents to fill in their email address at the end, to enter a lottery – thus, giving them the possibility to win a reward.

4.2 The Survey

This paper uses survey research to collect and analyze the data. This allows the assessment of the opinions of a wide range of people of different backgrounds. Moreover, it is possible to study how various factors may – or may not – influence personal online safety and overall opinions on the topic of surveillance and privacy. Survey research enabled the collection of responses from a large representation of backgrounds, ages, and nationalities, both inside and outside of the European Union. The wide range of respondents' backgrounds was chosen because, as Blank et al. (2014) explain, audiences which may be separate offline will unify in a single context online. As an example of this phenomenon, the authors describe the evolution of Facebook, which started as a social networking site exclusively for elite American university students, but has now become a "transnational network with more than 1.15 billion active monthly users of all ages" (p. 5). Therefore, people of all backgrounds are affected by questions of privacy and surveillance. More information on the case selection is mentioned in the following section.

The survey consisted of twelve questions of various lengths and was distributed electronically, through both Qualtrics and Google Forms[3]. The questions were divided into four parts. First, participants were asked about their personal use of online apps and websites. Then, the survey inquired upon their online safety measures. The third part had them rate various sentences in order to understand their opinions on surveillance, privacy, and selling data to third parties. The average completion time for this questionnaire was between five and seven minutes. Respondents moreover had the option to add extra comments following the twelve questions. Finally, participants were given the possibility to win a 15€ voucher once they had answered all the questions, by simply entering their email address at the end. This added an extra incentive for the respondents to finish filling out the questionnaire, and limited the amount of incomplete responses needing to be taken out of the analysis.

4.3 Case Selection

The aim of this survey was to gather 150 to 200 responses, which would allow for a wide range of respondents. At the same time, this amount of responses would lead to noticeable patterns. Originally, the survey was to be answered only by individuals born between 1985 and 2000. This range would have enabled a study a specific generation's opinions – the millennial generation – and it would have been interesting to see how growing up right before the internet versus alongside the internet could lead to diverging opinions on surveillance, privacy and security. However, in order to truly look into the impact of age on opinions and safety, the range was changed and anyone could take the questionnaire.

Demographic variables were included in the fourth section of the questionnaire. This included the

[3] The complete questionnaire is available upon request.

age of the respondents (which was later added into one of seven age categories), their gender, their nationality (later split into three different geographical regions – Europe, North America and East Asia), their highest level of education, and their employment status. In order to gather a representative sample, the survey was distributed through social media by six people belonging to three different age groups, and living in the three regions studied in this research. The aim of this sharing method was to ensure more diversity in the ages and nationalities of the respondents, all the while making sure that they had a regular online presence. Altogether, 164 responses were gathered over a weeklong period. Respondents were between the ages of 19 and 78, and came from 25 different countries.

5. Analysis

5.1 Age and Mistrust

The first hypothesis aims to understand if age has an important role in a person's degree of mistrust towards the Internet. Moreover, it attempts to uncover if age influences the likeliness of increasing privacy protecting measures online. H1 considers these two important elements separately. To facilitate the analysis, seven age groups were formed, in order to create fairly homogenous group sizes. Since the selected variables are ordinal, a correlation test is used to understand them. Correlation measures the association between two variables, which can have a positive, negative, or no relationship with each other. In this case, Spearman's coefficient is used to measure the relationship between age and degrees of mistrust, then age and individual measures to protect one's privacy. In order to assess the first part of this hypothesis, on the degree of mistrust, I selected six different sentences that the respondents were asked to rate on a scale of 'Strongly Disagree' to 'Strongly Agree':

(1) I have a clear opinion on surveillance issues;
(2) I believe surveillance needs to be taken seriously;
(3) I feel that surveillance is a violation to my intimacy;
(4) I feel spied on when I see targeted advertisement on my social media accounts;
(5) I am concerned about where my personal information may end up;
(6) I worry that my (future) employer might see my online profiles.

These sentences were used to estimate the mistrust or worries that individuals have online. Therefore they are used to measure, to some degree, personal concerns for privacy. In case of an association with age, this would show us whether younger or older respondents are more concerned about their individual privacy. However, after analyzing them with Spearman's coefficient, it appears that there is no relationship between any of these opinions and the age of the respondents. One can expect to have a clear relationship between variables only as long as the significance of the Spearman's coefficient is smaller than 0.05.

The second part of H1 brings up the different security measures that an individual can use to increase the protection of their privacy. Once again, age is the independent variable. The dependent variables consisted of six security measures, that the respondents had to rate on a scale ranging from "Never" to "Always":

(1) Do they always increase the privacy measures on an app as much as possible?
(2) How often do they read the terms and conditions when downloading a new app?
(3) Do they usually physically block the camera on their phone?

(4) Do they usually physically block the camera on their computer?
(5) Do they regularly delete their search history online?
(6) Do they generally avoid connecting new apps to their social media accounts?

These sentences are useful to assess if a particular age group is more likely to use certain privacy measures. Spearman's coefficient was again used to analyze a potential relationship between the variables. This time, two variables had a level of significance, as presented in the following table:

Table 1: Relationship Matrix: Influence of Age on undertaken Privacy Measures

Test	Significance[4]	Correlation	Relationship[5]
Measure: Physically block phone camera			
Spearman's coefficient	.027	.151	Weak positive relationship
Measure: Physically block computer camera			
Spearman's coefficient	.017	-.165	Weak negative relationship

The table shows that physically blocking a camera on both a phone and a computer (for example with a sticker) has a weak relationship with the age of the respondent. However, the direction of the relationship is different in each case. On the one hand, there is a weak positive relationship between age and the act of blocking the phone's camera. This means that the older the respondent, the more likely they will block their phone camera. On the other hand, age and the act of physically blocking a computer camera carry a weak negative relationship, suggesting that younger respondents are more likely to perform this action. The other four variables were shown to have no relationship with the age of a respondent.

To visualize the way generations address privacy related measures, a third test was conducted. This time, the ages were split into two groups: those ranging from 19 to 33 (the participants belonging to the 'millennial' generation) and those ranging from 34 to 78. Figure 1 shows how millennials vs. non-millennials answered the sentence "I increase privacy measures on the apps I use as much as possible." While millennials are more likely to 'always' increase these privacy measures (23.01% as opposed to 17.65%), the overall amount of respondents who answered 'always' or 'most of the time' or 'sometimes' was 84.96% for millennials and 78.43% for non-millennials.

On the other hand, the sentence "I read the terms and conditions when I download a new app" showed a more negative response. Indeed, as shown in Figure 2, both millennials and non-millennials tend to 'rarely' or 'never' read the terms and conditions, with 67.22% of the former and 56.80% of the latter generally avoiding this measure. This further shows that there does not seem to be an association between the respondent's generation and his or her use of security measures. Instead, it would appear that people generally preform similar types of security measures, regardless of their age.

[4] Significant at the <.05 level
[5] -1=perfect negative relationship; <-.6=strong negative relationship; <-.3=moderate negative relationship; <-.1=weak negative relationship; 0=no relationship; >.1=weak positive relationship; >.3=moderate positive relationship; >.6=strong positive relationship

H1 suggested that age was positively related to the degree of mistrust towards the Internet. However, it appears that age does not have a particular impact on people's relationship with online privacy.

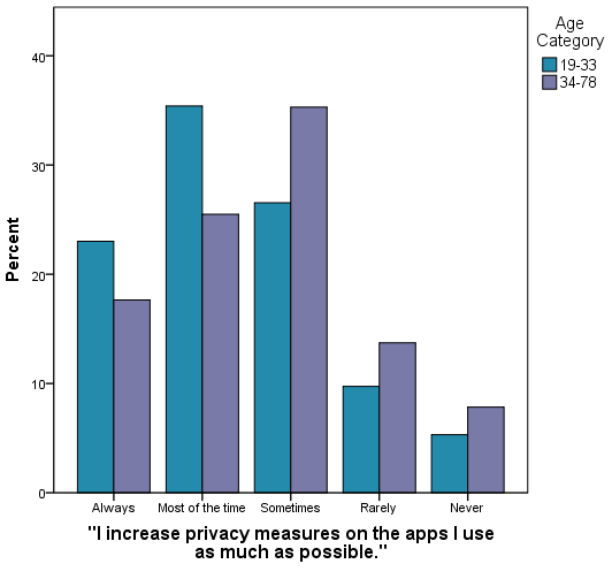

Figure 1: Generational Habits and Privacy – Increasing Privacy Measures[6]

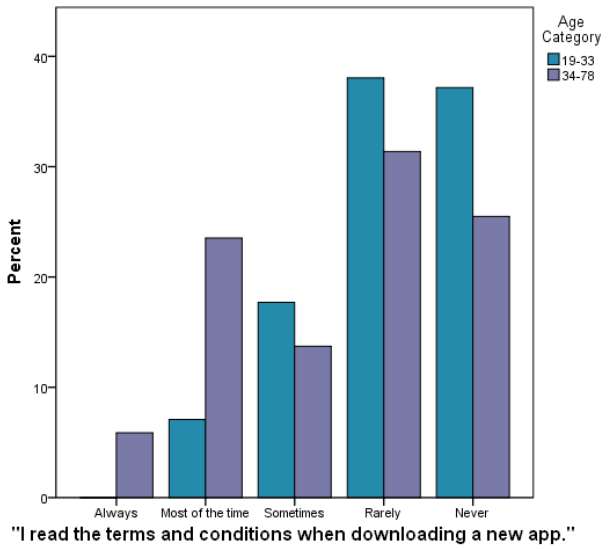

Figure 2: Generational Habits and Privacy – Reading Terms and Conditions

5.2 Usefulness and Yielding Data

The second hypothesis theorized on the relationship between an app's perceived usefulness, and the likeliness that a person would cede their personal information. To study H2, I first analyzed the responses

[6] All figures are based on the author's data.

to the opinion "Giving away my personal data is acceptable as long as an app is useful to me". The results appear in Figure 3.

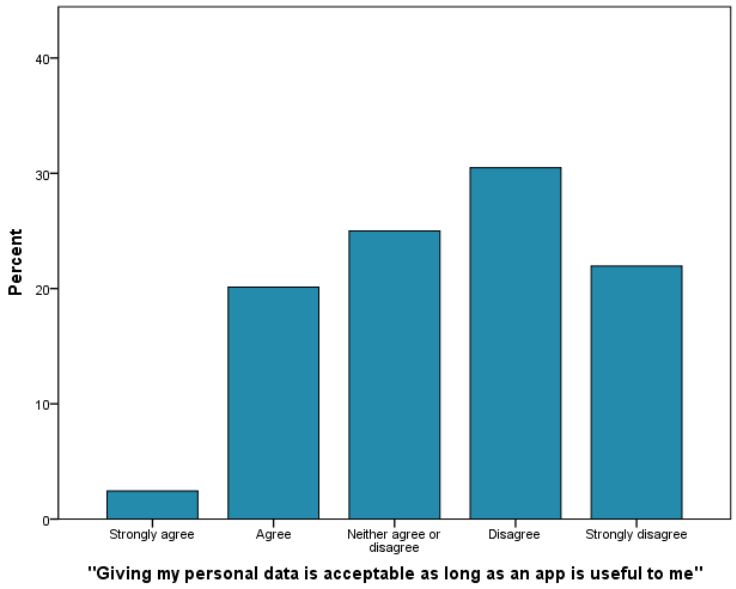

Figure 3: Usefulness vs. Privacy – Trading Data for Utility

Figure 3 shows that 52.44% of the respondents either disagreed or strongly disagreed with the statement; that 22.56% agreed or strongly agreed; and 25% did not have a particular opinion in one way or the other. While it appears that people do not want to trade their data for utility, a question emerges: How do people act in practice? The next step of the analysis of H2 is to look at the use and habits of certain types of apps. The first question of the survey asked respondents to select the types of apps they used at least on a weekly basis. Here, we assume that the apps people use frequently are those they consider the most useful in their daily lives. Question 5 later went back onto these categories, and had the respondents rate how likely they were to disclose their personal information for each type of app, on a scale going from 'Extremely Likely' to 'Extremely Unlikely'.

Thirteen app categories were given in the survey. The focus falls upon the four most commonly used among the respondents: messaging (used at least weekly by 152 of the 164 respondents), social media apps (147 respondents), music (102 respondents), and productivity (98 respondents). In addition, the use of fitness and health apps was examined. While it had a lower count of respondents (43 used these apps weekly), these types of apps generally call for users to give their personal data away more extensively than other categories. Indeed, to be of service to the user, these apps call for them to insert their age, height, weight, gender, and in some cases their diet and alcohol consumption. Altogether, the data could enable companies to draw a fairly accurate portrait of the user, their habits, their needs and their goals – all of which are ideal for targeted advertisement.

To assess how the frequent use of a certain app, and therefore its usefulness to the user, may affect the user's willingness to disclose personal information, a chi-square (X^2) analysis is applied. This type of analysis measures the significance – or lack thereof – between an independent and a dependent variable. An alpha level of $\alpha=.05$ for all chi-square analyses is used. In this case, it shows that there is an association between the two variables (in all categories, $.00 \leq p \leq .05$). The Cramer's V analysis shows that the association in all cases goes from medium to strong (see Table 2). Thus, the frequent use of a

certain type of app is rather strongly associated with the user's willingness to disclose their personal information, confirming H2.

Table 2: Association Matrix: Predicting Disclosures of Personal Information

Predictor Variable	Test	p-value[7]	Cramer's V	Strength of Association[8]
Disclosing Personal Information on *Messaging* Apps				
Usefulness to the user	X^2	.004	.304	Medium association
Disclosing Personal Information on *Social Media* Apps				
Usefulness to the user	X^2	.000	.364	Strong association
Disclosing Personal Information on *Music* Apps				
Usefulness to the user	X^2	.001	.339	Medium association
Disclosing Personal Information on *Productivity* Apps				
Usefulness to the user	X^2	.001	.348	Medium association
Disclosing Personal Information on *Fitness* Apps				
Usefulness to the user	X^2	.000	.385	Strong association

5.3 Rewards – Trading Data for a Bonus

Finally, H3 measures the degree to which people respond to rewards. This signifies that the possibility of gaining something would make people less wary of giving their data away. The way in which this hypothesis was studied is however rather unorthodox. Simply asking a question on rewards did not seem to be the most efficient or reliable way to examine the hypothesis. Instead, H3 was directly tied to the added incentive for the completion of the survey. It calculated how many people willingly gave their email address when being told that they would be entered to win a 15€ gift card[9]. In the end, 51.22% of the respondents entered their email address. This would suggest that people are neither likely nor unlikely to give away their personal information, and therefore does not confirm the hypothesis.

There is however one important limitation to the way the hypothesis was measured. The survey was on the topic of surveillance, so the respondents had in mind various questions that addressed the issues of privacy and data gathering. This limitation came through in several of the respondents extra

[7] Significant at the <.05 level
[8] <.1=very weak,.1-.25=weak, .25-.35=medium, .35-.45=strong, >.45=very strong
[9] The gift card was in fact real. Each email address entered by the time the survey was closed was given a number. A random generator was then used to produce a number, and the winner was contacted privately.

comments. Participants 58, 60 and 159 noted the irony of asking them privacy-related questions, while at the same time asking them for personally identifiable information. Participant 78 jokingly asked not to send her email address to interested third parties. Finally, Participant 16 noted that she had given real data about herself throughout the survey, and would not add an extra piece of information about herself by entering her email address, despite being interested in the voucher.

Measuring the third hypothesis proved to be difficult in this questionnaire. An option to gather more accurate, unbiased results would be to set a mock-survey on an unrelated topic, once again with the possibility to win a gift card. This method would allow to see how many people give their email when they do not have the topic of security and privacy freshly in mind. The problem with this is that the respondents to one survey might not match those of the second, and it would not be possible to associate any of the privacy questions with the likeliness to cede their email.

5.4 Final Remarks

Many other dilemmas and paradoxes appear in the field of surveillance, which would need to be studied more in depth. For instance, one paradox is that of opinion – potentially disproving the idea that individuals with stronger opinions on privacy and surveillance are more likely to increase their online security and privacy measures. Moreover, despite data breaches, people still consistently use the same social networking sites. It would be interesting to analyze the reasons behind this. This study also only briefly touched upon demographic characteristics outside of age. A more in depth research on gender, employment status, education level, and nationality would allow the understanding on whether or not certain groups are more likely to worry about surveillance concerns. Finally, some of the participants' extra comments proved to be interesting and enlightening, and brought forward some different perspectives. Conducting interviews alongside the survey simultaneously could consequently further the reasoning behind certain attitudes and opinions.

6. Conclusion

The Internet has transformed our daily lives and our perceptions of privacy. Society has become more focused on surveillance; individual awareness on data gathering has grown. Yet at the same time, and quite paradoxically, the boom of social media networks and apps of all kinds caused people to lower their guard. We now share many details of our lives online, through pictures, group forums, and by joining various websites and apps. While there are concerns over government surveillance, it is far easier to follow society and let our personal information fall into amorphous flows of data (Zurawski, 2011). However, recent scandals have brought surveillance into question.

This study aimed to reveal some of the reasons that keep people from striking a balance between privacy and surveillance in an online setting. It brought forward the paradoxes and dilemmas that people encounter, which make the topic of privacy remarkably multifaceted. The survey provided a greater understanding of the respondents' individual habits and how they may be affected by their views on privacy and surveillance. It showed that age does not have a great impact on people's thoughts on online safety, nor on the measures they might undertake to protect their privacy – thus going against the popular belief that younger people do not care about privacy as much as their older counterparts. Moreover, it exposed the inconsistency between certain opinions and matching actions. Indeed, while the survey's respondents generally claimed not to be willing to accept giving their data in exchange for a useful app, they acted

otherwise. Using an app regularly was strongly associated with the tendency to disclose personal information. Finally, it attempted to test how the participants responded to rewards, or in this case, the possibility of a reward. This experiment would however need to be redone, outside of a surveillance-related survey, in order to get more reliable and unbiased results. Altogether, the survey brought interesting results and analyzing it brought forward possibilities for further research.

Further research could additionally be done on the measures people take not only to protect themselves from surveillance, but to actively resist it. Resistance would start with simply re-appropriating the concept and adjusting the manner in which we look at surveillance. Playful systems, as have been studied by Gangneux (2014), Chen (2008) and Koskela and Mäkinen (2016), are also a mean of resistance. They exploit a system that usually exploits us. Furthermore, it addresses the stigma of privacy invasion. As such, game-like approaches would take away some of the worrying elements of surveillance, instead making it participatory and entertaining. Using games and a lighter approach to tackle surveillance may be considered just a small tactic rather than full-blown resistance, yet these actions allow the surveillance process to be challenged. Raising awareness on issues of privacy would be more effective if carried out in a less threatening manner. Nevertheless, responses to surveillance are much more complex than a simple acceptance versus resistance binary.

Tables:

Figures: