Do the advantages of giving up our privacy outweigh the possibilities that an entity might abuse of this power?

Ingy Nazif
Do the advantages of giving up our privacy outweigh the possibilities that an entity might abuse of this power?

Ingy H Nazif

Spring 2014

Dr. Sherin Darwish
Acknowledgments

I would like to express my gratitude to Professor Darwish, my research supervisor, for her guidance and valuable suggestions.

I would also like express my thanks to Mr Phillip Sewell, who assisted me in sharing the survey.

Finally, I would like to extend my thanks to my family and to Ramy Hamza for their support.
Table of Contents

Acknowledgments 2

Abstract 4

Introduction 5

Literary Review 6
  Advantages and the Right to Privacy 6
  How to Safeguard our Privacy 7
  The Issue of Trust 9
  The Abuse of Personal Data 12
  The Role of Media 16
  Limitations 18
  Conclusion 18

Methodology 20

Results 21
  The survey for university students 21
  The survey for working adults: 29

Discussion 37
  Analysis 37
  Limitations 44

Conclusion 45

References 47

Appendices 48
  Appendix A: Protecting personal data in a digital age (Survey for University Students) 48
  Appendix BI: Protecting personal data in modern societies (Survey for Working Adults) 50
  Appendix BII: Protéger nos informations personnelles dans les sociétés modernes (Survey for Working Adults in French) 53
Abstract

This paper explores how modern-day societies become dependent on surveillance through cameras and online social networks. This research aims to prove how young generations would rather accept the loss of privacy rather than taking decisive action to protect privacy. At first with the analysis of articles concerning risk perception, the legal status of privacy, and the typical media discourses about privacy. The method used in this research is primary research, through a survey given to two samples: University students and working adults. However the results are expected to be difficult to discuss since the samples are very different in age, social class, culture and education. This paper examines the perception difference between young generations and older generations, as well as the abuse that may occur if surveillance becomes too widespread to propose that additional research be conducted to attempt to find possible legal or practical methods to limit surveillance in a reasonable way.

Keywords: privacy, surveillance, security, risk perception.
Introduction

Security is a vague notion for most people. Do the advantages of giving up our privacy outweigh the possibilities that an entity might abuse of this power?

Cryptography and many types of security issues have always fascinated this researcher. She proposes to research into how security may affect our privacy and our well-being. What this researcher means by security is the procedure to keep personal information or valuable objects out of the reach of potentially ill-intentioned individuals. Moreover, she will discuss the issues of encryptions have become part of our daily routine, should it be for accessing our computer or our mobile phone or our email account. Nowadays, we struggle with two types of security: online security (a bank account for example) and physical security (the placing surveillance cameras).

This study mostly looks into the issue of balancing security and privacy. In fact, we find a lot of articles about the Patriot Act and privacy, or Facebook and privacy. But very few sources cover how the extensive or extreme use of security actually leads to vulnerability because we entrust our personal information to accounts protected by passwords, or through encrypted messages.

However, the purpose of this paper is to show how this trust is inflated by misperceptions encouraged by the media. Governments and certain groups can leak information that can be used against us (to insurance companies for example). This research intends to convey the idea that all the information given online can be used in a way most information providers do not realize. This researcher will show that just like in a court, whatever you write will be used against you.
**Literary Review**

**Advantages and the Right to Privacy**

Some argue that privacy is a privilege but should not be considered a right. However, this researcher believes that privacy is a right. In his thesis, Olivier Proust, Graduate Department of the Faculty of Law, from the University of Toronto, initially, he sets the scene with background information and defines the key concepts of his research. One of these key concepts is privacy in which he explains how some philosophers such as Hegel, have come up with a definition of the moral status as a reflection of the corporate order in which an individual might find himself. Proust explains how the “corporate view” as he calls it opposes the right of privacy (Proust, 2002).

However, he argues against this view by presenting the definition given by the British-American philosophy, which exposes privacy as a right that should be protected and that is a natural right, because it defines the legitimacy of a political structure through the private and individual judgments (2002). In fact, Guirguis, a Doctor of Philosophy at Auburn University, references Epicurus (Guirguis, 2001) who also mentions that privacy is deeply tied to our nature. He explains that we are affected by outer constraints on our inner freedom and that opposing this inner freedom prevents us of developing ourselves and making creative or different choices. Hence, this supports the claim that privacy is a fundamental and natural right. It is essential to us as it gives us the chance to flourish internally and intellectually.

These papers are valid in their claims because this researcher feels that the corporate view is not quite accurate, that is, that privacy and the individual’s moral status depends on the political structure to which we belong, on the society and the place we hold in it; this means that privacy is an artificial right, not a universal one, but a fabricated need which
changes from society to society and from social class to social class. In fact, this researcher believes that privacy is essential in the sense that it gives us a time to be spontaneous and relaxed. In other words, that a private environment gives us a space to think differently, to be different and to be creative.

Hence, it is important to understand the value of privacy. In his thesis, Magued F. Guirguis, (2001) discusses the significance of privacy. He divides his argument into two parts: the value of privacy for the individual, and the value of privacy for the society. As for the first part, he argues that informational privacy need not be valued only for inadequate information to the public. In fact, he claims that being able to let go of the strain of being who we should be, in private moments is essential: it’s the only time during which we can really be spontaneous. He gives the example of a police officer who should not express emotions on the job but can with his family. However, he explains in the second part that the right to privacy is also essential to society: on one hand, because it is so closely related with some freedoms. And on the other, he supports the idea that the lack of privacy impedes creativity, hence, impedes progress (Guirguis, 2001).

This example reveals how stressful our daily “public” life can be but how our intimate environment help to balance out our lives. Therefore, this researcher claims that privacy is an undeniable right and a valuable right. But is also a way to measure the potential of progress of a society. Thus, we must attempt to protect our privacy as much as we can: to be able to conserve our personal freedoms and an environment in which we can relax without worrying about formality and decorum.

**How to Safeguard our Privacy**

Besides, after this researcher has made clear how important privacy is, then it is equally important to be able to safeguard it. In his thesis, Proust, mainly argues against the
Patriot Act. He analyses the circumstances in which the Patriot Act was accepted and its implications regarding the right of privacy. However, he mentions cryptography as a possible solution to regain our privacy and explains in detail how programs such as Carnivore, that Intelligence Agencies use to “filter” the Internet traffic works (Proust, 2002).

In fact, modern day protocols of encryption provide almost total protection against cipher text-only attacks, since the modern standards are now secure against brute force. In other words, it would take too much time to recover the message by this method. Hence, the only way for the attacker to recover the message is by knowing the key somehow. To this effect, it is important to clarify that Intelligence agents do not spend their time reading all the Internet traffic (messages, blog posts, emails, etc.). Proust stresses how they use programs like Carnivore: filtering using keywords, which means that a message not containing any of the keywords should not be picked up by Carnivore (Proust, 2002).

However, protection against eavesdropping using encryption protocols also implies limitations. In his thesis, Guirguis, discusses the rational limitations of personal freedom. He also supports his argument with varied cases and defines precisely the legal position for privacy in email, phones and video, focusing on the United States. He mainly examines the legal and ethical issues brought up by governmental surveillance. One of the points he makes is that we need to put rational limitations to our privacy (Guirguis, 2001).

In fact, it is clear that if the government has no way of observing what citizens do on the Internet, this network becomes the perfect place to design the perfect crime in total impunity. The other issue is that users of the Internet seem unaware of both the dangers of exposing to much information online (some employees have been dismissed because of Facebook posts), and the possible ways of protecting themselves from this danger. Then it would be useful to campaign for informational privacy.
The Issue of Trust

It is clear that there has been a very important decrease in the importance given to privacy, especially in the younger generations. In fact, this decline, Judith Rauhofer, a professor at the University of Edinburgh, argues (Rauhofer, 2008), is due to users’ perception of the risks of not safeguarding our privacy. In her article, Rauhofer explains how we perceive personified risks as greater than anonymous risk; she quotes Stalin: “a single death is a tragedy, a million deaths is a statistic”. She cites Schneier to this effect by explaining that the perceived risk of an earthquake is bigger than the perceived risk of slipping on the bathroom floor: although more people die because of the latter (Schneier, 2003: 26–27). She points out that it is because an earthquake is a rare but spectacular event and because we cannot control the earthquake. Whereas, entering the bathroom is a risk we take willingly (Rauhofer, 2008). Hence, the perceived risk might not be accurate, which is clearly the case for privacy. In other words, humans have a tendency to exaggerate some risks while being indifferent to others that may be important such as daily car accidents which kill thousands of people, as opposed to the one bombing that takes a few lives. As a bomb explosion that potentially kills hundreds of people, but because driving is a risk that we willingly take, we tend to downplay the risks. Whereas with an event we cannot control, such as an electric storm, we tend to overemphasize the risk factor.

Another point Rauhofer makes (Rauhofer, 2008) is that citizens are trading their privacy for other values such as security, our relationships with others. Moreover, citizens in the United States and the UK trust the state more than they trust fellow citizens. She concludes her article with the idea that CCTV (Closed-circuit Television) did not prevent thefts and assaults. Even though it made it easier to find the criminals (Rauhofer, 2008). Hence, this researcher feels that, disregarding whether CCTV is an invasion of privacy or not, this new technology did partially meet it’s primary objective: preventing crimes.
It is clear that it did not meet it entirely, as Rauhofer points out people are still getting assaulted. But this researcher would object that she does not mention where the crimes happen. It is unclear whether the assaults continue to occur in the range of the cameras or not. In other words, this researcher feels that instead of totally preventing crimes CCTV has just shifted the crime locations. Thus, that a criminal instead of stealing someone in front of the camera will look for a place without cameras to steal, but it doesn’t mean that overall no crimes have been prevented. In fact, this researcher believes that CCTV makes it harder for individuals to commit crimes by observing a certain public space and collecting video footage that may serve to find a criminal.

However, the researcher sees there is another problem CCTV does not solve but may emphasize: social sorting. When looking at the footage, policemen will tend to consider some minorities or social classes more ‘suspect’ (Muslims or Dark skin individuals in Europe for example). But this issue does not reveal itself only with surveillance cameras, but through Facebook. An employer may decide to look up one of his employees on Facebook (or any social network) and if he finds out through the groups the employee belongs to that he is part of a religious minority for example; he can decide to dismiss him. Thus, when we give information about our religious or political beliefs in a social network can become a problem, considering that anyone can find this information.

During last semester (Fall 2013), in a scientific thinking general lecture, the video of Dave “an amazing mind-reader” was brought up to make us think about social media. A man pretending he is a mind reader (Dave) and actually gets people to come to be interviewed, in Belgium. He tells each invitee personal information about him (the invitee), and each person seems amazed. After he is finished telling them all about their lives and personal issues he explains to them how he knows, Facebook. He explains to them that they should really watch out because all their lives are accessible from the Internet.
Neglecting the fact that Facebook sells personal information to the authorities, another treacherous characteristic of Facebook are friends. In fact, friends of friends are able to view information (such as our names, address, the workplace or educational place) but our friends might add on Facebook people they’ve met at most for one day, or people they have never even met in real life. In the example of Dave he reveals very personal information, such as bankrupt or the death of a family member etc.

Actually, the information posted on Facebook can turn against us if an ill-intentioned person uses it. Hence, we must be aware of it to protect ourselves. Here I mentioned Facebook but the same problem occurs for many other social networks and for our devices. Most of us carry with us everywhere a credit card, a mobile phone, maybe a tablet and/ or a personal computer. However, each one of these devices sends data to the servers informing them of our precise location. The moment someone uses his credit card or get a call, the bank and the police are informed of his location.

Since the UK and US governments centralize the data, it makes it easier to collect an almost complete set of information for every individual. In his article, Frank Bannister, from the Trinity College in Dublin, explains how it is risky to cede our privacy to the state and explains the different means of surveillance and mentions data mining (the combination of data to deduce possible intentions of individuals). He also explains through which methods the state can access personal data: third parties and public services. Individuals give personal information to third parties (banks, insurance, etc.) and to public services (parking, health) voluntarily and knowingly. However, these third parties often choose to exchange, sell or give private information to the government, which raises the issue of trust (Bannister, 2005).

The article of Bannister displays the prominence of data flow between third parties and the government for which we are not consulted. Furthermore, in this article, Neil Richards, a professor of Law in the Washington University, mainly explains the necessity of
a better definition of why surveillance is harmful. Richards also points out that surveillance is not just an issue of so-called “autocratic” states. In fact, complex alliances exist between the government and the private sector that exchange data. The government may get data from an insurance company and in return give them information about the way their clients drive thanks to radars for example (Richards, 2013).

In fact, this is not a problem encountered only in so-called autocratic states, it is quite disturbing that these examples stress the point that our trust is scarcely justified since in most democratic states, the private and public sectors companies are under governmental control. It is reasonable that the companies should be somehow under the control of the government so that they are subject to sanitary or social standards. For this reason, it is important that the surveillance goes both ways: from the government to the citizens, and from the citizens to the government. If citizens don’t watch the government closely, it will soon become corrupt, which leads to the paradox quote: “Quis custodiet ipsos custodes?” (“Who guards the guards?”, Juvenal, around the end of the first century AD).

**The Abuse of Personal Data**

The Panopticon (in Greek: observation of all) is a model of prison conceptualized by Jeremy Berntham in the late XVIIIth century. However, it is interesting to note that many prisons have included elements of Berntham’s designs but none reflected his designs entirely. In the center of the building there is the watchtower from which the guards can watch the inmates. This way the prisoners themselves are unable to know if they are watched, creating a sense of omnipresence. In fact, Rauhofer makes the point (Rauhofer, 2008) that nowadays: our modern societies have become very similar to that model, as long as citizens know that their personal information might be consulted at anytime without their permission.
As a matter of fact, as a concept, the Panopticon may seem brilliant, it would be cheap to implement since there would be few guards and the prisoners will be seen as a workforce. Hence, the director will have an interest in having his prisoners alive which is important since in most prisons the mortality rates are very high. But this type of design also serves to psychologically reform the supposed criminals. In other words, the fact that the prisoners know they can be watched at all times will make them more incline to abide by the rules and therefore hypothetically making them better people. Actually, the ideas behind the Panopticon are arguably not that inhuman, however this researcher objects that the lack of privacy required for this model is excessive. The inmate has not a moment to himself, not a moment to relax, to say what he wishes and do what he wants. In the researcher’s opinion, this lack of privacy would lead to brainwashed inmates that have no creativity.

As is shows in the writings of Vasari, a contemporary of Leonardo Da Vinci, it seems the famous Renaissance man was very concerned by his privacy, since he wrote in a way only he could understand. Interestingly, he wrote in Italian but instead of writing from left to right, he wrote from right to left as if with a mirror (Vasari, 1508). This example, in the
opinion of the researcher is not an example of egoism since most of the sketches drawn by Da Vinci are still used till today for anatomy reference. But it is an example of an artist who wanted to keep his notes private, just as people now communicate with encrypted messages. The objective is the same: establishing a private conversation accessible only to the sender and the recipient.

Our present societies are now more and more concerned about terrorism, with the September 11\textsuperscript{th} attacks, and the rise of occurrences of bomblings. In his book, O’Neil, a professor at the Department of Politics in the Government University of Puget Sound, Tacoma, explains the notion of complex systems, complicated networks that are essential to every country, the challenge now is preventing these complexes from being used for another purpose (O’Neil, 2005). In the case of the 11\textsuperscript{th} of September, the complex that was used for terrorism is aircraft, which was not intended to be a weapon. Yet, by using the two airplanes, the terrorists have been able to do substantial damage and considerable human loss. It shows a new potential source of danger, and implies that it might not only come from weapons and elaborated equipment but very simple material that can be subverted. It is really sad to realize that since what people care about most is knowing how much victims there were, then the top news are the most deadly. Hence, the objective of terrorists becomes oriented in terms of victims to hit the top pages in the media. In other words, to be heard of, the terrorists aim to take away the maximum possible of lives.

In another section of this book, O’Neil revokes (2005) the idea that biometrics could actually be implementable and efficient, because they store the information and data in a centralized database. With the development of face recognition, the risk is that the supposed “authority” is able to access an array of personal data, which could be dangerous for the individual since it may be subject to abuse (O’Neil, 2005). What it means is that linking a person to all the data related to him/her such as insurance details, work profile, biometric
information, or pictures, in a unique database is dangerous for this person. In other words, if an ill-intentioned person accesses these large quantities of grouped data, the consequences for the person the data describes could be fatal.

In our modern societies, information is a weapon, which leads scandals because of the revealing of a fraud or affair. A very common example is blackmailing, if an ill-intentioned individual possesses “secret” information that could potentially ruin the career of someone else, this individual could blackmail him/her or put him/her in danger. But then what exactly should we protect? Thus an essential issue we have not addressed yet is the definition of personal data.

Christopher Millard, a former President of the International Federation of Computer Law Associations, and Kuan Hon, is a Research Assistant, Cloud Legal Project, at the University of London, focus on the gap between the European directives concerning personal data and how it is interpreted in England (Millard & Hon, 2011). The main point they make is that: if the definition of personal data is not clear, how do we restrict unsolicited access to our personal information legally? This article also shows how on this point England has much narrower view of personal data than the rest of Europe, which basically means that there is more data concerning individuals that is considered as legally accessible (Millard & Hon, 2011). In the researcher’s opinion, this article is interesting because it recaps the evolution of the notion of personal data legally. However, it gives possible solutions to bridge the EU and UK legal standards but the authors do not come up with a more precise definition themselves, because it is so problematic.

Through this example, it is clear that the issue of defining personal data is addressed differently depending on the culture and the society. However, our perception of privacy issues and governmental surveillance are heavily influenced by the image that is given of
them in the media. In other words, if a channel tends to present CCTV as efficient for example, then most of viewers of this channel will tend to have a positive opinion regarding CCTV.

**The Role of Media**

It is arguable that the media tends to be Manichean, sometimes highlight surveillance as being highly efficient and beneficial, and occasionally criticizing these measures. In his article, David Barnard-Wills, a Senior Research Analyst in Trilateral Research & Consulting at Cranfield University, explains (2011) how he went through the process of collecting articles to compare their way of presenting the information. He argues that there are two main discourses: one of them displaying surveillance as useful against crime and terrorism, the other showing surveillance as an abuse and as an attempt to personal liberties.

In this context, Barnard-Wills proceeds by applying different frames of analysis: the economic impact, the human impact, the “them” and “us” divisions, the control by powerful others and moral values. For each frame he exposes what one discourse argues versus the other discourse. This article explains how media plays in important role in the acceptance of new security measures such as surveillance, in this case in the UK. Moreover, Barnard-Wills justifies his stance by explaining that media can have a controlling or manipulating effect on it’s audience and that it is important to pay attention to how things are exposed (Barnard-Wills, 2011). The table that sums up the differences in the discourses relative to the frame (Barnard-Wills, 2011):
In the researcher’s opinion, it is important to understand these discourses to be able to understand to point of view of most scholars on surveillance. In fact, they too are subject to this influence. When reading these articles, it is easy to see that they represent either one of the discourses and very rarely in the positive discourse. This researcher would like to comment that it is much easier to find an academic article criticizing surveillance than one praising it. Actually, it seems that condemning governmental surveillance is quite in vogue. The only article this researcher found that tries to have a more objective point of view is the one written by Guirguis (2001). He is the only one to evoke the concept of rational limitations to our ideas and the idea of balance. In other words, he says that we must admit that governmental control is important for our societies as well, but it is also important to consider preserving our rights in a reasonable way. We can’t expect to be in a perfect society where no one is corrupt, and where we don’t need any order to do justice.

For this reason, we need to look for a compromise, and we need to try to be more objective about our opinions. What this researcher means is that we must stay reasonable and try to not just follow the ideas in the media, we must think for ourselves. Surveillance is not
black nor white, it depends where and why it is applied, who applies it, and there are many arguments to support or criticize it. The same applies for privacy, we cannot permit ourselves to condemn how an employer or a policeman react to the pages we like and the groups we join, on social networks. As users we must start seeing social networks as a public space, if we don’t want to face social sorting because of political or religious beliefs we must keep those to ourselves or reserve them to real life conversations.

**Limitations**

This researcher first intended to prove that security creates vulnerability; that the more we try to surround ourselves with barriers the more we make breaches in them. In the example of CCTV, it is supposed to represent more security for the citizens. However, the video footage could be transformed and used in a totally different purpose and be turned against one or a group of citizens should they be innocent or guilty. This researcher was forced into shifting this initial claim to be able to find adequate sources. Another limitation to this paper is that the researcher was unable to encounter a reliable resource presenting cases of data abuse, which weakens her argument about the “potential” danger of centralized data.

Another hurdle this researcher must consider is that she also is subject to media influence. Hence, her opinion may be biased because of the experiences she has lived and the information she was given.

**Conclusion**

In brief, this researcher has presented how difficult it is to define concepts such as privacy and personal data, and most importantly privacy’s value for society as a whole and for each individual. She has also explained how physical and online security are becoming challenges for both the government and the citizens, as well as in terms of law. In fact, most countries do not agree on agree on what can be legally accessible to a policeman and what
cannot, such as the UK and the European Union (Millard & Hon, 2011). This is the reason for which we need to know how online surveillance programs work and how we can protect ourselves, with cryptography for example (Proust, 2002).

However, we also need to be aware of the fact that people and Internet users and now trading privacy for their relationships with others, to be able to use social networks. Actually, we have a distorted perception of risk, and it is noticeable that we should still try to preserve our privacy even if we have “nothing to hide”. Privacy is not just an excuse for the criminals (Rauhofer, 2008). Another point that needed clarification is that defending our privacy is not just an issue of non-democratic states, and the way each device we use is able to accumulate and link our personal data and accounts makes it more dangerous for us. Especially when countries decide to establish a “data alliance”, that gives them the possibility to spy on their citizens through another country (Bannister, 2005).

The other very important concept concerning surveillance and privacy is the panopticon, which shows the potential power of surveillance and the sense of omnipresence. However, the panopticon has become concept we can use to describe our modern societies (Rauhofer, 2008). Moreover, in our current societies, most of our opinions and most of what we say is shaped and informed by the media, which gives the media the power to manipulate and influence us, pushing us to extremes (Barnard-Wills, 2011). We either tend to see the government and the US as a modern-day “Big Brother” as described by George Orwell, or we see the extreme measures such as biometrics and extensive video surveillance as a step to establish security.

This is what makes this researcher think that the more we try to protect ourselves from each other by letting the government take over our privacy and in the same time we want to keep our secrets as foolishly as the objects we “possess”, the more we are making
ourselves exposed to personified attacks. If we hang on to our “precious” objects too desperately we can end up losing our lives and the objects with it. As in the story of a millionaire in Sub-Saharan Africa who owned a Mercedes with a fingerprint lock, a group of criminals stopped his car killed him to take his finger and his car. Or as in the book *Angels & Demons* by Dan Brown, in which the criminal has to kill to be able to access what he wants because of an iris scanner. Thus, this researcher believes we should never be pushed to extremes, to this effect I cite Horace, who many years before her said: “aurea mediocritas” (“the golden middle”, 1st century BC). **So how beneficial is it really to give up our privacy to social media, private and public companies?**

### Methodology

Before collecting the data and answering the surveys, all the respondents were clearly notified that the information and answers acquired are strictly for academic analysis and research purposes. The research methods used hold no threat to the respondents, it is free of any physical, or psychological harm, they participated under their own will and consent.

For the purpose of this research, the method used was experimental. The objective of these surveys was to test the following hypothesis: older generations are more attached to privacy than younger generations who tend to trade privacy for better social connections and national security, Internet users (young and old) are, for most, unaware of the tracking of their personal data, behaviors and interests. Two different surveys were sent out to different samples: one was sent to approximately 180 university students, and the other to about 80 adults. However, only a total of 38 students responded to the survey and about 30 adults only responded. This researcher interests' were to know if the perception of privacy is different for working adults and young adults (university students). The other issue that will be explored through the surveys is the risk perception and awareness of both students and adults. How
aware are they of the risk they take when they post personal information on social media? How do they react to direct/physical surveillance?

The issue of privacy is becoming more and more important with the placing of cameras above ATMs, on highways, in front of supermarkets... A research done in the UK estimates that there is about one camera for 32 citizens. However, it seems people have not really done anything against it. Do people feel too helpless in our fast-evolving societies? Are young citizens and netizens just not aware? Or do they see privacy as not being important compared to national security? These are some of the question this researcher will address by distributing the surveys, collecting and analyzing the data.

Results

I conducted two slightly different surveys to support the main claims of this research paper, which are that:

- Younger generations are noticeably more reluctant than older generations concerning the issue of privacy.

- That most of the Internet users and modern citizens accept easily the idea of sharing personal information, which could be used in an unexpected and undesirable way.

The survey for university students

The aim of my first question (see chart A) was to get a better representation of the sample by asking in what country they were studying. Fortunately, I was able to reach quite a few different countries. A little more than 60% of the respondents study in Egypt, a little less than 30% study in France, one respondent studies in Canada, another studies in Nepal and one of the respondents skipped this question.
The next question (see chart B) tests how they perceive the concept of privacy. Interestingly, 45% of the surveyed students answered that privacy is “the advantage of keeping some information personal”, 37% answered that it is the “right to choose what to share”, while, 8% expect privacy to be the right to be let alone, 5% hold the view that privacy isn’t meaningful anymore, and one respondent added in the other section that everybody defines privacy in the way each one finds best.
The third question’s purpose is to give me an idea of how neglectful young generations can be when it comes to agreeing to terms and conditions in a responsible manner (see chart C). In fact, exactly 50% of the sample claim that they have read the terms and conditions at least once before installing a new program or operating system. Thus, the other 50% admits that they never read the Terms and Conditions before installing a program.

The fourth question (see chart D) was intended to find what kind of personal information do young generations willingly share over the Internet. 33 out of 38 respondents answered they did not mind sharing their nationality, almost as much respondents (32) accept to share their gender, 25 accept to share their full birth date, and 21 would share their job. However, only 12 would share their religion, 10 would share their relationship status and only 5 would share their political views openly. Then only one respondent for each would accept to share his/her mobile phone, his/her sexual orientation and his/her education. On the other hand, one of the respondents answered that he or she would share nothing at all.
The fifth question explores the reaction of university students if cameras were monitoring them in their university (see chart E1). For this question, on one hand, 25 out of 38 answered it was acceptable as long as it is for the security of the students, 18 would not appreciate or hate being monitored but would not do anything about it. On the other hand, 5 claim that there is no way of stopping it and 7 claim that it is totally normal or that they already are in a public space. Then I grouped the respondents into two groups: those clearly would not take any decisive action against this, and those that would do something about it. It turns out that more than 85% would not take any action against the implementing of surveillance in their university and only 15% would resist to the monitoring (see chart E2).
The two next questions explore the awareness of Internet users by asking them if they have heard of cookies and if they know what they are (see chart F and charts G1 and G2). For the first of the two questions about 75% of the respondents answered they’ve heard of cookies before, hence, almost 25% of the respondents have never heard of cookies (chart F). The second question proposes different definitions of cookies. To this question 19 respondents have chosen the first possible definition which is that cookies are small amounts of data that create a preference profile for each netizen, 16 answered that cookies sent their information to third parties and advertisement companies, only 10 knew that cookies saved usernames and passwords, and only 4 knew that cookies saved their shopping cart on e-commerce websites, 10 others saw this name before but do not know what cookies are and 10 respondents answered that they had no idea what cookies were and 1 last respondent answered he could not remember (see chart G1). Here it is interesting to note that all the functions or definitions of cookies proposed were correct. This gives me the opportunity to answer the question: for those who know what cookies are, how much do they know about them? Then I grouped the answers of the respondents who didn’t know what cookies were and group those of those who knew what they were and it turns out that a little less than half the respondents knew what cookies were and a little more than half didn’t know what they were (see chart G2).

![Chart F: Have you ever heard about cookies?](image)
The next question was meant to evaluate how much netizens think they are vulnerable, and to what extent. In fact, the question supposed a fictitious random person who knew the respondent’s name and searched as much information as possible. The respondents were then asked how much information they thought the person could find about them. 3 respondents answered that the supposed person would only find 10% of his information, 3 others answered 20%, then 10 respondents answered the person would only find 30% of their information, then 3 answered 40%, 5 respondents answered 50%, and 8 respondents answered 60%, 2 answered 70%, 3 of them answered 80%, none of them answered 90% and only one of them answered 100% (see chat H1). So too make these results clearer and easier
to read, I group the answers that said that the supposed person would find 50% or less information about them and I group the others together. In fact, more than 60% of the respondents claim the person would not find more than 50% of the information about them, and only a bit less than 40% evaluate their informational vulnerability at more than 50% (see chart H2).

The next question was to test the awareness of the respondents concerning governmental surveillance. So they were asked if they thought intelligence agencies could access absolutely all the information they had online. About 40% answered that intelligence agencies could for security purposes, almost 25% answered they were not sure, 18% gave other answers, 11% answered “Of course they can”, 5% answered “yes they can” and surprisingly none of them answered that intelligence agencies could not access all their personal information online (see chart I1). Therefore, I decided to group all the respondents
who were not sure, all those who justified the power of intelligence agencies by saying that they were responsible for the security. In fact, I found that 0% thought intelligence agencies couldn’t access the information, 24% were not sure, 42% justified it with security and 34% agreed that intelligence agencies could access the information but did not necessarily appreciate it and justify it (chart I2).

![Chart I1: Do you think Intelligence agencies can access all the information you post online?](image1)

![Chart I2: Do you think Intelligence agencies can access all the information you post online?](image2)

Finally, the last question was to test the opinion and critical analysis of the respondents. They were asked how they thought the media presented privacy. On one side, 10 respondents answered that the media presented privacy as not important compared to national security, while 11 answered that the media presented privacy as being very
important and a basic human right. On the other side, 11 respondents answered that the media presented privacy in a biased way while only 5 thought the media presented privacy in an objective way. However, most of the respondents (15) agreed that the media tended to present privacy as either very important or as unimportant (see chart J).

![Chart J: Do you think that the media presents privacy:](chart)

The survey for working adults:

The first question (see chart I) tests how they perceive the concept of privacy. Interestingly 18% of the surveyed students answered that privacy is “the advantage of keeping some information personal”, 61% answered that it is the “right to choose what to share”, while, 15% expect privacy to be “the right to be let alone”, none hold the view that privacy isn’t meaningful anymore, and one respondent added in the other section that privacy corresponded to the first three definitions (“the right to choose what to share”, “the advantage of keeping some information personal” and “the right to be let alone”).
The second question’s purpose is to compare the sense of responsibility between older and younger generations when it comes to agreeing to terms and conditions (see chart II). In fact, 39% of the sample claim that they have read the terms and conditions at least once before installing a new program or operating system. Thus, the other 61% admits that they never read the Terms and Conditions before installing a program.

The third question (see chart III) was intended to find what kind of personal information do older generations, supposedly more aware and responsible, willingly share over the Internet. 26 out of 33 respondents answered they did not mind sharing their nationality, almost as much respondents (25) accept to share their gender, 21 accept to share...
their full birth date, and 16 would share their job. However, none would share their religion, 11 would share their relationship status and only 2 would share their political views openly. Then only 2 respondents would accept to share his/her mobile phone, and another would share his/her educational degrees. On the other hand, one of the respondents answered that he or she would not share the same information depending on the social media.

The fourth question explores the reaction of working adults if cameras were monitoring them in their workspace (see chart IVA). For this question, on one hand, only 11 out of 33 answered it was acceptable as long as it is for the security of the students, 10 would not appreciate or hate being monitored but would not do anything about it. On the other hand, none claim that there is no way of stopping it and none claim that it is totally normal, one reports that cameras have already been installed in his workspace, and another claims he would look for another place to work in. Then I grouped the respondents into two groups: those clearly would not take any decisive action against this, and those that would do something about it. It turns out that more than 61% would not take any action against the implementing of surveillance in their university and 39% would resist to the monitoring (see chart IVB).
The two next questions explore the awareness of Internet users by asking them if they have heard of cookies and if they know what they are (see chart V and charts VIA and VIB). For the first of the two questions 97% of the respondents answered they’ve heard of cookies before, hence, only 3% of the respondents have never heard of cookies (chart V). The second question proposes different definitions of cookies. To this question 16 respondents have chosen the first possible definition which is that cookies are small amounts of data that create a preference profile for each netizen, 14 answered that cookies sent their information to third parties and advertisement companies, only 4 knew that cookies saved usernames and passwords, and 6 knew that cookies saved their shopping cart on e-commerce websites, 6 others saw this name before but do not know what cookies are and 2 respondents answered that they had no idea what cookies were (see chart VIA). Here it is interesting to note that all the functions or definitions of cookies proposed were correct. This gives me the opportunity
to answer the question: for those who know what cookies are, how much do they know about them? Then I grouped the answers of the respondents who didn’t know what cookies were and group those of those who knew what they were and it turns out that about 75% knew what cookies were and a little less than 25% didn’t know what they were (see chart VIB).
The next question was meant to evaluate how much netizens think they are vulnerable, and to what extent. In fact, the question supposed a fictitious random person who knew the respondent’s name and searched as much information as possible. The respondents were then asked how much information they thought the person could find about them. I respondent answered that the supposed person would only find 10% of his information, none answered 20%, then 7 respondents answered the person would only find 30% of their information, then 5 answered 40%, 7 respondents answered 50%, and 5 respondents answered 60%, 4 answered 70%, 2 of them answered 80%, none of them answered 90% and two of them answered 100% (see chat VIIA). So too make these results clearer and easier to read, I group the answers that said that the supposed person would find 50% or less information about them and I group the others together. In fact, more than 60% of the respondents claim the person would not find more than 50% of the information about them, and only a bit less than 40% evaluate their informational vulnerability at more than 50% (see
The next question was to test the awareness of the respondents concerning governmental surveillance. So they were asked if they thought intelligence agencies could access absolutely all the information they had online. About 50% answered that intelligence agencies could for security purposes, a third of the sample answered they were not sure, 12% gave other answers, surprisingly only of them answered that intelligence agencies could not access all their personal information online because his/her accounts were protected by password (see chart VIIIA). Therefore, I decided to group all the respondents who were not sure, all those who justified the power of intelligence agencies by saying that they were responsible for the security. In fact, I found that 3% thought intelligence agencies couldn’t access the information, 33% were not sure, 52% justified it with security and 12% agreed that intelligence agencies could access the information but did not necessarily appreciate it and justify it (chart VIIIB).
The next question was meant to assess how exposed respondents thought one of their most private accounts of working adults (bank accounts) was. In fact, only two respondents out of 33 expect their bank account to be totally private; 7 respondents expect their bank account to be 20% to 30% private; none expect it to be of 40%. However, 5 respondents expect their bank account to be 50% private and one respondent answered that he thought his bank account is 60% private. Meanwhile, 4 respondents claim the privacy of their bank account is of about 70%, 5 estimate it at 80%, 5 other estimate it at 90% and 4 respondents estimate their bank account to be totally private. Hence, 24 out of 33 respondents (73%) estimate the privacy of their bank account to be higher or equal to 50%. Whereas, only 9 out of 33 respondents (27%) estimate that their bank account is less than 50% private (see chart IX).

![Chart IX: How private do you think the information on your bank account is?](chart)

Finally, the last question was to test the opinion and critical analysis of the respondents. They were asked how they thought the media presented privacy. On one side, 8 respondents answered that the media presented privacy as not important compared to national security, one of them commenting that the media presented privacy as an obsolete concept (translated), while 6 answered that the media presented privacy as being very important and a basic human right. On the other side, 13 respondents answered that the media presented
privacy in a biased way while only 1 thought the media presented privacy in an objective way. However, 10 respondents agreed that the media tended to present privacy as either very important or as unimportant, one of them commenting in the other section that the media presented privacy in a “In a hypocritical way, calling “scandal” when government agencies are accused of invading privacy but … forgetting the way that journalists … hound families and individuals for a story”. Whereas, 2 respondents answered that it depended on the country and the media, another yet, answered he/she didn’t know (see chart X).

<table>
<thead>
<tr>
<th>Chart X: Do you think that the media presents privacy:</th>
</tr>
</thead>
<tbody>
<tr>
<td>In an objective way, 1</td>
</tr>
<tr>
<td>As very important because it's a basic human right, 6</td>
</tr>
<tr>
<td>As not important compared to national security, 8</td>
</tr>
<tr>
<td>In a biased way, 13</td>
</tr>
<tr>
<td>As either very important, or not important, 9</td>
</tr>
<tr>
<td>Other, 5</td>
</tr>
</tbody>
</table>

**Discussion**

**Analysis**

The way the survey was conducted was to highlight potential differences between the perception and sense of responsibility of two different age categories. In the first question it is interesting to note that older generations tend to perceive privacy as being the freedom of choosing what to share, while younger generations tend to see privacy as the advantage of keeping some information personal. Hence, older generations may tend to see privacy as a
sort of control of their personal information, whereas, younger respondents try to retain some information, which does not imply having full control on their personal information.

However, the results to the second question (if respondents had ever read the terms and conditions) seem to contradict my claim. In fact, the results show that 50% of the younger respondents have never read the terms and conditions, whereas a little more than 60% of the older respondents, supposedly more responsible, admitted they have never read the terms and conditions. This is a surprising result that seems to contradict the results to the first question as well. The reasons why we tend to neglect the importance of the terms and conditions are that they are long and they are not easy to read, but also because of the problem of risk perception as mentioned by Rauhofer (Rauhofer, 2008). In fact, users tend to think that many others have accepted the conditions and nothing happened to them so why would something happen to them? Someone must have read them; if there was anything wrong with the terms and conditions they would know. It is important to notice that 60% and 50% are very high percentages of users accepting terms and conditions without reading them, in a supposedly well educated sample.

In the third question (which asked what information the respondents would agree to share), there are two interesting observations to make. The first is that nationality, gender and birth date seem to be the most commonly shared type of information and it the same order for young and older generations. The second is that the older category seems to be much more reserved when it comes to more detailed information such as political and religious views. In the younger sample, 12 respondents answered they would share their religious views and 5 would share their political views. Whereas in the older sample, none would share their religious views and only 2 would share their political views. Thus, older generations seem to act more responsibly or with more precaution than younger generations.
The fourth question asked how respondents would react, if their employer or their university (depending on the age category) decided to set cameras in the workplace or the university. It is interesting to notice that for the younger category most of them either chose that it was acceptable as long as it was for the security of the students (25 out of 38 respondents) or that they would not like it but that they would not do anything about it (17 out of 38). Whereas, in the older category only 11 out of 33 answered it would be acceptable, and only 10 answered they would not like but they would accept it, and surprisingly, 12 out of 33 answered they would protest against it. It is interesting to notice that only 5 would protest in the sample of the younger category, the same number of respondents think we can’t stop the loss of our privacy by the installing of cameras, and 5 respondents out of 38 answered that it would be normal. However, in the older sample, none of the respondents answered that it would be normal or that there is no way of stopping the installing of cameras, even though one of them commented there already are cameras in his workplace.

When regrouping the information, it is clear that more than 50% in each sample would not take decisive action against the cameras. For the younger category, a little less than 90% would not do anything about it, and for the older category a little more than 60% would not take action against the placing of the cameras. Hence, we see the obvious difference, the older generations are much more willing to fight for their rights, whereas according to these results, younger generations tend to accept to let go of their privacy more easily. This supports my first hypothesis about younger generations. In fact, it is arguable that older generations have not been affected the way younger generations are by the extreme ways the media presents privacy. Barnard-Wills explains that by observing the articles that mentioned privacy in the last few of years, it is obvious that the two main points of view have been getting more and more extreme over time (Barnard-Wills, 2011). He basically presents these two Manichaean points of view: one that displays privacy as being an unnecessary
advantage that is not as important as national security, and the other displays privacy as being absolutely essential and a right we have to fight for (Barnard-Wills, 2011). Thus, younger generations would have a tendency to be influenced by this bias and would tend to go for the first point of view which is much more common, especially after September 11th.

Furthermore, in the ninth question dealing with how media presents privacy, it is interesting to see that in the younger respondents’ category the “either as important or as unimportant” (15 out of 38) answer was the most chosen, which reflects the two extremes mentioned earlier. Additionally, it is also surprising to see that almost the same number of respondents answered that the media presented privacy: “as not important” (11 out of 38) or “as important” (10 out of 38). Likewise, the younger respondents seem to agree somewhat that the media presents the subject in a biased way (11 respondents) rather than in an objective way (5 respondents). However, as for the older category, the answers “as not important”(8 respondents out of 33) and “as important”(6 respondents) still keep a fair balance. But the idea that the media presents the subject in a biased way (13 out of 33) was the most chosen answer, only one respondent answered that the media is objective about it. Yet, they don’t seem to feel the presence of two dominating points of view the way the younger respondents did: 9 out of 33 respondents answered that the media presented privacy “as either very important, or not important”, and they mention that it might be different from a country to another and from a media to another. Thus, this supports my claim in the sense that the two extreme points of view seem to appear quite clearly, confirming the article by Barnard-Wills (2011).

The results of the fifth question (asking if respondents have heard about cookies) seem rather intriguing. In fact, it turns out about only 75% respondents of the younger category have heard of cookies. Whereas, 97% of the older generations have heard of them, only one respondent answered he had not heard about cookies. Which is surprising recalling
the results obtained for the second question about the terms and conditions, in which the younger category apparently read the terms and conditions more often than older respondents. Hence, even though younger respondents tend to read the terms and conditions more often than older respondents, they apparently are not as well informed on the technicalities of surveillance. But, in the eighth question, it is surprising to notice that younger respondents appear to be much more sure of surveillance than older respondents. In fact, about three quarters of the younger sample is sure that intelligence agencies can access everything they post, and the remaining quarter is not sure whether they can access their files or not. Whereas, in the older sample about a third are not sure and only 64% are sure they are being monitored. Thus, younger generations seem more aware that they are being watched but might not exactly understand how.

However, I assumed respondents would be less aware of technicalities such as cookies. Thus, this makes Rauhofer’s argument about biased risk perception more valid (Rauhofer, 2008). The users seem to be aware that there is a potential danger but underestimate this risk because they take it willingly (Rauhofer, 2008). This hypothesis seems to fit with the situation: younger respondents but also older respondents take the risk for most (50% and 61%) of not reading the terms and conditions, although they seem aware of the potential abuse that could happen knowing that intelligence agencies or others can access their personal data but they still take the risk. Yet, when asked how private they thought their bank accounts were in the last question: most of the working adults considered that it was more than 50% private (a little more that 70% of 33 respondents), even if they had just answered that intelligence agencies could access all their personal information. Moreover, it is important to notice the unexpected percentage of respondents who are not sure whether intelligence agencies can access their information or not, even though the sample reached is supposedly well educated.
Returning to the cookies the sixth question was meant to differentiate the people who have heard of cookies and know what they are and those who have heard of them but don’t know what they are. Actually, it is quite obvious that most of the respondents perceive cookies as being small amounts of data that create a preference profile for each user (19 out of 38 for the older category, and 16 out of 33 for the younger category) and as being small elements that send their data to third parties (16 for the working adults, and 14 as for the university students). Nonetheless, only 10 out of 38 of the university students and only 4 out of 33 of the working adults knew that they stored usernames and passwords. Yet, very few of respondents knew that cookies also stored the information for shopping carts on e-commerce websites (4 of the younger category, and 6 in the older category).

Thus, cookies are mostly perceived as small elements that track all you do and send your information without your consent, which is true, but there’s more than this to cookies. Only very few respondents answered that they also save the shopping carts and usernames and passwords. Still, there are quite a few respondents who admit either having no idea about what cookies are (10 in the younger sample, and 2 in the older), or having seen the name but still not knowing what they are (10 in the younger sample and 6 in the older sample). Therefore, about 1 out of 4 university student has come across the word cookie but does not know what they are, and a little more than 1 out of 6 working adult is in the same situation. It seems that Internet are either are not curious enough to understand how they are tracked. These results seem to confirm my first hypothesis, which is that younger generations tend to be less preoccupied by the issue of privacy.

As for the seventh question, it asked the respondents (on a scale from 0 to 100%) how much information they thought a random person would be able to find about them just using their names. To this question, surprisingly, the answers of the two categories are very similar: about 40% of the samples estimated the supposed person would find 50% or less of their
personal information, and about 60% estimated that the supposed person would find more than 50% of their personal data. Recalling the results to the question that asked what kind of information they would share, the two samples answered very differently the older sample being more reserved. However, it is important to notice the slight difference in distribution: in the graph for the younger sample, the distribution was closer to the 50% and less, whereas in the graph representing the older sample has a distribution closer to the center. In fact, this shows that younger respondents tend to share more information and expect a random person to find a little less than of their personal information compared to older respondents who tend to share less information and expect the same amount of information to be found. In fact, every little piece of information leads to another, as shown in the video starring Dave (Unknown, 2012). In the video, Dave shows how much he can find about people just by finding their names on Facebook (Unknown, 2012).

In fact, a name supposes a nationality and/or location, a man called Tom will more likely be living in Australia, England or the United-States, whereas a man called Mohamed will more likely by living in the Arab World. A location may suppose activities through which the supposed person can connect with the “victim”. If the “victim” posts his phone number the “searcher” can know where he is, in which country at least, and at most his exact location at any time. If the victim posts his/her political or religious views maybe subject to monitoring or social profiling by the authorities or by his/her employer. If pictures are available on the victim’s profile, the searcher may be tempted into other plans especially if it is a woman or a child. But the pictures also reveal who are the victim’s closest friends, if the victim is in a relationship, a great deal of the victim’s personality as well. If the victim accepts many friends without being careful enough chances are the searcher may have a mutual friend with victim. This means the victims’ posts, pictures, information about the job,
the pages the victim likes become even more accessible, revealing an array of additional information.

Hence, with very little information about one person it is easy to find a lot more, especially if the victim does not change his/her privacy settings often enough. Internet users seem to consider themselves secure and aware of the potential dangers of exposing their information over the Internet, however it seems this perception is biased. Moreover, it certainly seems they are somewhat aware of the way the media manipulates the information creating two extreme and opposite discourses about the issue of privacy.

Limitations

The perception of privacy and surveillance is very possibly affected by the culture. An English citizen who sees surveillance cameras very often will very probably not react the same way as an Egyptian, if a new item of surveillance is introduced in his daily “sphere” (the public spaces he would visit daily). Hence, the sample I was able to reach is not representative of a global perception, and in fact, it seems difficult to generalize a perception over so many different societies, traditions and cultures. However, I was able to reach at least two very different populations: 60% of the respondents were Egyptian and about 30% were French. Whereas, the majority of the second sample was French (20 respondents answered the survey in French and 13 the survey in English). This may be reflected in the answers to the question about the media and privacy. It is likely that because of what Egyptians have through in the last four years, they are more aware of the how the information can be manipulated in the media.

Another limitation faced was that I did not know enough English-speaking adults, hence, I had to come up with a French version of the survey. This cost me time when I translated it and when I came to analyze the results I had to retranslate everything in English again. Thus, the questions and answers have been translated and might not yield exactly the
same meaning as in English. It is regrettable that I only had a semester to complete this research and was only able to give out the survey for a week, which also limited the number of respondents making it not as valid as it would have been if it had been conducted in parallel in several countries under the same conditions. In fact, the respondents I was able to reach are mostly from the middle-upper class which makes the answer not representative of either countries, or cultures.

**Conclusion**

Finally, this research has served the purpose of giving an overview of the concepts of privacy, risk perception and surveillance. After having conducted the surveys and analyzing the results, this researcher has realized that the results seem somewhat contradictory and it is difficult to point out clearly which of the two categories (university students and working adults) is more responsible and more aware of the way they make themselves more vulnerable with each piece of information they share.

This researcher thought Internet users let out so much information because they are not aware that someone can research it. It turns that even if between 25% and 33% of the respondents are not sure about it, the majority are aware that their information is accessible. Thus, the article by Rauhofer provided a better answer: they are aware but they are trading their privacy and freedom for better social relationships, because their risk perception is biased and this bias is encouraged by the media (Rauhofer, 2008).

Conversely, Benjamin Franklin is often quoted as saying: “People willing to trade their freedom for temporary security deserve neither and will lose both” (18th century). This quotes exposes the paradox in a more condensed way: by accepting to give up their personal freedom for the sake of security, when it comes to online surveillance through social media or physical surveillance through cameras, Internet users are exposing themselves more and
will lose their privacy (part of their freedom) and security because of the way the government can abuse of the personal data they share.

Furthermore, this researcher would definitely recommend that more in-depth research be done, on a wider scale. But also, with more representative samples of the Internet community throughout the world and with samples targeting the citizens exposed to video surveillance, to reflect on why citizens accept to be monitored and what impact it can have on their personal freedoms and security over the long run. This researcher also believes that it is important to do more research about the fragile link between security, freedom, and insecurity. She started this research in the idea that this is a subject that can be resolved by logic and a topic she already knew about, she then realized how little she knew and how much more there is to research in this field. Ultimately, this researcher would like to recall the very famous quote of Socrates, conveyed by Plato: “ἕν οἶδα ὁτι οὐδὲν οἶδα”* (3rd century BC).

* The one thing I know is that I know nothing.
References


Illustrations:


Appendices

Appendix A: Protecting personal data in a digital age (Survey for University Students)

Dear respondent, this survey aims to find out more about the perception of privacy in young adults and their willingness to preserve their privacy. The information collected is confidential and is gathered only for research purposes under the supervision of my rhetoric professor Dr Darwish. Kindly be aware that I will need to have collected the data by May 10th 2014. This survey contains a total of 10 short questions. You may decide to abandon the survey at any moment, and your response will not be taken into account. Thank you for your time.

1. What country are you studying in?
2. How would you define privacy?
   - The right to be let alone
   - The right to choose what to share
   - The advantage of keeping some information personal
   - Privacy isn’t meaningful anymore
   - Other
3. Have you ever read social networks’ privacy policies when signing up?
   - Yes
   - No
4. What personal information would you agree to share on a social network?
   - Nationality
   - Gender
   - Date of birth (full)
   - Job
- Religious views
- Relationship status
- Political views
- Mobile phone number
- Home Address
- Other

5. If your university decided to put cameras on campus how would you react?
   - This is totally normal
   - It's acceptable as long as it is for the security of the students
   - I would not appreciate it, but I would accept it
   - I would protest against such an intrusion to our privacy
   - There's no way of stopping it
   - Other

6. Have you ever heard about cookies?
   - Yes
   - No

7. Do you think cookies are:
   - They're small amounts of data that is stored by the website to customize the pages I visit and create my preference profile
   - They save my usernames and passwords for a website
   - They send my information to third parties without my consent
   - They save shopping cart on e-commerce websites
   - I saw this name somewhere in the privacy settings, but I don't know what they are
   - I have no idea what they are
8. How much information do you think a random person could find out about you only knowing your name?
   (On a scale from 0% to 100%)

9. Do you think Intelligence agencies can access all the information you post online?
   • No it's impossible, emails and inboxes are meant to be private
   • They can but that's for security purposes
   • They can't, my accounts are protected by a password
   • I'm not sure
   • Other

10. Do you think that the media presents privacy:
   • As not important compared to national security
   • As very important because it's a basic human right
   • In an objective way
   • In a biased way
   • As either very important, or not important
   • Other

Appendix B1: Protecting personal data in modern societies (Survey for Working Adults)

Dear respondent, this is survey aims to find out more about the perception of privacy in working adults and their willingness to preserve their privacy. The information collected is confidential and is gathered only for research purposes under the supervision of my rhetoric professor Dr Darwish. Kindly be aware that I will need to have collected the data by May 13th 2014. This survey contains a total of 10 short questions. You may decide to abandon the
survey at any moment, and your response will not be taken into account. Thank you for your time.

1. How would you define privacy?
   - The right to be let alone
   - The right to choose what to share
   - The advantage of keeping some information personal
   - Privacy isn't meaningful anymore
   - Other

2. Have you ever read social networks' privacy policies when signing up?
   - Yes
   - No

3. What personal information would you agree to share on a social network?
   - Nationality
   - Gender
   - Date of birth (full)
   - Job
   - Religious views
   - Relationship status
   - Political views
   - Mobile phone number
   - Home Address
   - Other

4. If your employer decided to put cameras in your workplace how would you react?
   - This is totally normal
   - It's acceptable as long as it is for the security of the students
- I would not appreciate it, but I would accept it
- I would protest against such an intrusion to our privacy
- There's no way of stopping it
- Non-applicable
- Other

5. Have you ever heard about cookies?
   - Yes
   - No

6. Do you think cookies are:
   - They're small amounts of data that is stored by the website to customize the pages I visit and create my preference profile
   - They save my usernames and passwords for a website
   - They send my information to third parties without my consent
   - They save shopping cart on e-commerce websites
   - I saw this name somewhere in the privacy settings, but I don't know what they are
   - I have no idea what they are
   - Other

7. How much information do you think a random person could find out about you only knowing your name?
   (On a scale from 0% to 100%)

8. Do you think Intelligence agencies can access all the information you post online?
   - No it's impossible, emails and inboxes are meant to be private
   - They can but that's for security purposes
   - They can't, my accounts are protected by a password
• I'm not sure
• Other

9. Do you think that the media presents privacy:
   • As not important compared to national security
   • As very important because it's a basic human right
   • In an objective way
   • In a biased way
   • As either very important, or not important
   • Other

10. How private do you think the information on your bank account is?
    (On a scale from 0% to 100%)

Appendix BII: Protéger nos informations personnelles dans les sociétés modernes
(Survey for Working Adults in French)

Ce questionnaire a pour but de découvrir et d'avoir une meilleure idée de la perception
de la vie privée chez les adultes et de leur détermination à la protéger. Les informations
obtenues sont confidentielles et ne serviront qu’à un projet de recherche, encadré par mon
professeur de rhétorique Sherin Darwish. Sachez par ailleurs qu’il m'est nécessaire de
finaliser les résultats avant le 13 Mai 2014. Ce questionnaire contient un total de 10 questions
brèves qui ne vous demanderont que peu de temps. Vous pouvez aussi décider d'abandonner
le questionnaire à tout moment; vos réponses ne seront alors pas incluses dans ce projet.
Merci de votre aide et de votre attention.

1. Comment définiriez-vous la vie privée?
   • Le droit d'être laissé tranquille
   • L'avantage de pouvoir garder quelques informations personnelles
• Le droit de choisir ce que l'on partage
• Le concept de vie privée n'a plus vraiment de sens maintenant
• Autre

2. Avez-vous déjà lu les conditions générales que vous acceptez?
   • Oui
   • Non

3. Quelles sont les informations personnelles que vous accepteriez de partager?
   • Date de naissance (en entier)
   • Nationalité
   • Statut de relation (en couple, seul(e), ou marié(e))
   • Sexe
   • Adresse de votre maison
   • Numéro de téléphone portable
   • Travail
   • Opinions religieuses
   • Opinions politiques
   • Autre

4. Si votre employeur décidait de placer des caméras de surveillance dans votre lieu de travail, comment réagiriez vous?
   • C'est tout à fait normal
   • C'est acceptable tant que c'est pour garantir la sécurité
   • Je ne l'apprécierais pas mais je l'accepterais
   • Je revendiquerais mes droits face à une telle atteinte à ma vie privée
   • Il n'y a aucun moyen de l'arrêter
   • Ne peut pas me concerner
5. Avez-vous déjà entendu parler de cookies?
   - Oui
   - Non

6. Vous pensez que des cookies sont:
   - Ce sont des petites quantités d'information qui sont mises en mémoire par les sites pour adapter les pages que j'ouvre en fonction du profil de préférence que les compagnies publicitaires m'ont attribué
   - Ils sauvegardent mes noms d'utilisateurs et mots de passe pour un site
   - Ils envoient des informations me concernant à d'autres organisations sans mon autorisation explicite
   - Ils sauvegardent mon panier de courses sur des sites de e-commerce
   - J'ai déjà vu ce terme quelque part mais je ne sais pas trop à quoi cela correspond
   - Je n'ai aucune idée de ce que c'est
   - Autre

7. Quelle quantité d'information vous concernant pensez-vous que quelqu'un pourrait trouver juste en connaissant votre nom?
   (Sur une échelle de 0% à 100%)

8. Pensez-vous que les services de renseignement peuvent accéder à toutes les informations que vous mettez en ligne?
   - Non c'est impossible, les emails et les inbox ont été créés pour être privés
   - Oui ils peuvent, mais c'est pour des raisons de sécurité
   - Non ils ne peuvent pas, mes comptes sont protégés par des mots de passe
   - Je ne suis pas sûr(e)
   - Autre
9. Pensez-vous que les médias présentent la vie privée:

- Comme étant négligeable comparée à la sécurité nationale
- Comme très importante parce que c'est un droit fondamental
- De manière impartiale
- De manière non-impartiale
- Soit comme très importante soit comme négligeable
- Autre

10. Dans quelle mesure pensez-vous que votre compte bancaire est privé?

(Sur une échelle de 0% à 100%)