IDSI 31421 - Sem IDS:Applied Cybersecurity

June 26, 2016

Jaubert Quentin, Zamora Adrien

Final Group Deliverable: Privacy on the Internet: a sweet dream?

"Big Brother is watching you" wrote Georges Orwell in his book named *1984* (published in 1949). In this groundbreaking book, Orwell describes a society in which the officials know everything that would happen inside the country by performing an omnipresent surveillance over the inhabitants. Today's police forces and secret services own a numerous number of surveillance tools - such as biometry, chips, facial recognition, localisation - that allow them to become very intrusive security forces. But the "policing" has now also become the property of major private companies (social media platforms, search engines, telecommunication carriers etc). A funny way of rethinking Orwell's quote in our modern world would be: "*Big Browser is watching you*".

There was a time where people had their privacy. One could go shopping when exiting the office, buy several stuffs in cash, go back home, close the doors and curtains, and run their private life. That was it. But privacy has evolved over time. If "privacy" can be defined as a "right to be let alone" (Warren and Brandeis, 1890), or even "the right to prevent the disclosure of personal information to others" (Westin, 1967), the concept has recently taken a multidimensional nature regarding "information, accessibility and expression" (Decew, 1997), and with the rise of the Internet, technology has created new privacy issues (Austin 2003) which lead us to wonder: is online privacy a sweet dream?

In order to understand the issues linked to our online privacy and generate insights from it, we adopted the following method:

- How has the privacy concept evolved with the appearance of the Internet?
- In such a connected world, should we/can we protect our privacy? If yes, how?
- Where will we be standing in the next 5, 10, 20 years? Will "online privacy" ever mean anything in the next decades?

I. How has the privacy concept evolved with the appearance of the Internet?

The concept of “Privacy” appeared in the late nineteenth century in the Western Countries. Indeed the creation of privacy followed the development of the urbanization of those countries. When you lived in a little town, the other inhabitants of the village knew everything on you and vice versa. The only privacy you had was perhaps the intimate relationships with your wife/ husband. The building of cities have allowed people to become strangers one to each other. One doesn’t know their neighbours and can do whatever they want at home. Of course, some other kind of surveillance/information retrieval could be set up (ex: police forces would use bugs, listen to the telephone). Still, most people could enjoy freely their private life. The twentieth century was the privacy golden age.

Over the past twenty years and with the democratization of the Internet, this vision of privacy was deeply challenged and modified. Generally speaking, the increased ability to gather and send information has always had negative implications for retaining privacy. The more you give information to your browser, the more it knows (about) you. In his article *The Web means the end of forgetting* (2010), professor Jeff Rosen explains that we have now entered a new age “where every online photo, status update, Twitter post and blog entry by and about us can be stored forever”. The problem of course is that you don’t really know where your information is kept. You don’t really have practical means to know who has access to your data. This could explain why you shouldn’t use Google, Facebook, Twitter… But. actually Google has recently given the right to desactivate any type of cookies / past searches that it would use to offer personal advertising solutions.

The notion of privacy in our society is constantly moving, and a pair of 21st century developments — the birth of Internet-based social networks and the rise of anti-terrorism snooping by the government — are wrecking traditional expectations and confounding social scientists. The decline of privacy reflects the rise of technology in Western life. Our phones are now mini-computers, with cameras and a wireless connection to the Internet that make it possible for us to text, email and tweet photos/videos around the Web. While most social media users know about the dangers of protecting passwords and viruses, many have no idea that there is danger in being trigger-happy on social networks. These problems include everything from personal safety and identity theft to potential difficulties in the workplace from an ill-advised tweet or Instagram photo. For many social network users, the potential loss of privacy is often outweighed by the desire to connect with other people online, especially because they find it easier to make connections and maintain relationships.

And when it comes to relationships… The 30 million users of AshleyMadison.com also thought they had some privacy – until hackers exposed their names, addresses and credit card payments. Unlike the almost routine reports about electronic thefts of financial data, this led to

more serious consequences (two suicides were linked to the disclosures...). Along with recent high-profile breaches that have affected retailers like Target and government agencies like the IRS and Office of Personnel Management, the Ashley Madison hack shows online information is never truly safe, despite people's increasing willingness to hand it over.

People are aware of this situation and would even be willing to ask for money for the use of their personal data by a third-party. Why should I let Facebook, Google, Netflix or any website using my cookies the right to make money on my back/my online behaviour? How could I monetize my private data?

Dave Eggers, in his book *The Circle (2016)*, describes one solution to this problem. The current numerical world is based on a situation where you accept to give personal information in exchange to the access to free products or applications. Another trend relies on the creation of web contents based on your personal success. This is the Youtube effect. Anyone can become a star on Youtube and earn money from the platform by gathering a great number of fans. Youtube's basic remuneration system follows this motto: "The more viewers watch your video, the more money you get". To do so, one widespread piece of advice is to give always more personal insights to viewers. The more intimate the video, the more success it might get. This explains for example the incredible amount of unboxing videos (that consist of the opening of a makeup or a shoe box with precise descriptions).

The privacy concept has deeply evolved within the past decade. While the trend during the last century was to be always more private, the rise of the Internet has completely modified the vision of our privacy we have had. New devices linked with an increase of web surfing have created a new world in which everyone exchanges freely a lot of personal information. Is this situation desirable?

II. In such a connected world, should we and can we protect our privacy? If yes, how?

Websites can collect various types of information, such as voluntarily provided information which may include our name, address, email address, billing/credit card information etc., as well as information automatically collected when visiting the websites, which may refer to cookies, third party tracking technologies and server logs. Even though personal information is said to be knowingly and willingly collected, through surveys, completed membership forms, or emails, websites tend to gather anonymous demographic information and other personal/non-personal information, such as age, gender, household income, political affiliation, race and religion. It is even possible for websites to collect information about our computer hardware/software. Such collected information may include our IP address, browser type, domain name, access time and various website addresses.

The result to that is that we live in a world where we are forced to give personal information against our will. In many cities, we are filmed by video cameras in train stations, airports, streets, taxi a large number of times each day without even knowing it. Our phone can be bugged very easily by police forces and we are never sure messages are not checked before we receive them. For instance, if you spend a certain amount of time in Dubai and you happen to “criticize” once the laws or the government, your future Whatsapp messages will automatically be read by public officials before being sent on your phone. One real issue on that subject is that people also tend to accept this situation without contestation.

However, public forces are not the most dangerous spies anymore. Many other actors dealing with our data have replaced them. For example, when using a traditional Internet access, my telecommunication carrier is one of the first companies I have to deal with. Should I trust him in retaining my personal surfing data? The browsers also belong to that group of potential spies. Should I trust Google? I should also take an insurance against the potential uses of cookies on the websites I visit. J. Edgar Hooper and the CIA were dreaming about it, Facebook has done it. Sex, name, surname, age, religion, photo, location, friends, relations and so much more information (such as bank accounts, medical treatments etc). Some might wonder about the underlying goals of this kind of multinational company. Eventually, do I sufficiently trust all those firms to be secure enough not to be hacked by potential distrustful groups of people who could then pressure me?

All those potential threats give us interesting insights about how we should try to protect our privacy online. Can we do it? Aren't we too subject to those major websites good will? Actually, a great number of recent evolutions might give us hope towards this situation.

First and foremost, the Big Number Law might be interesting to assess the efficiency and seriousness of those websites. For example, since Facebook gathers a great number of users and makes a lot of revenues from it, the company can hire the best IT and cybersecurity teams and prevent themselves from a potential breach in their systems. What is more, as those technological firms are in the spotlight, they cannot make any mistake. If they were reselling our personal data to a third-party, public opinion would quickly be aware of it and would soon manage to make them change their policy.

Second, from a legal point of view, numerous privacy laws aiming at protecting and preserving the privacy rights of the individuals (and especially privacy laws on the Internet) have been enacted over the past few years. The Data Protection Regulation offers the same legal scheme for all members of the European Union. Internet users are protected against clandestine usage and illegal use of their personal data. Basically, if anyone uses your name or picture in a message you don't recognize yourself in, you have the right to ask for erasing this post. Furthermore, the right to forget is deeply inscribed in the law and major online firms should comply with it. Finally, various consumer NGOs intend to point out the flaws in major websites policies in order for those companies to modify them.

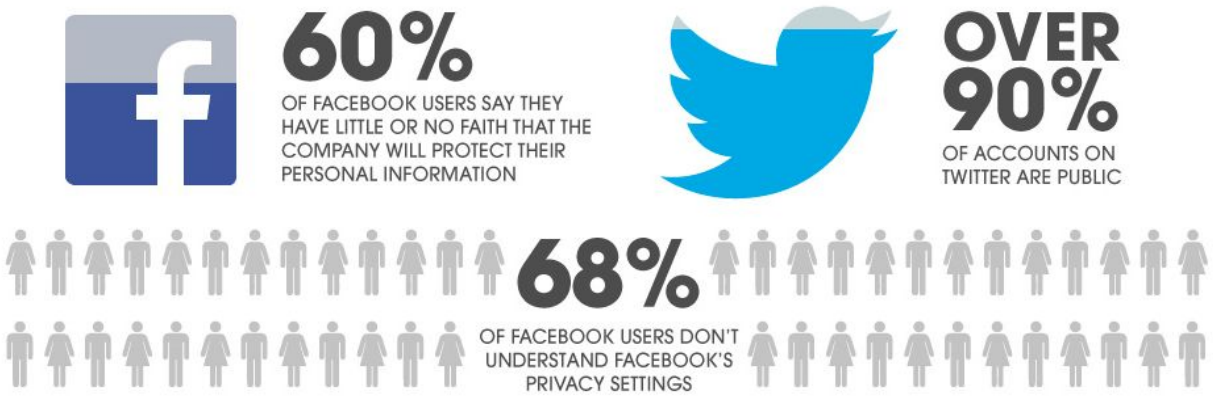
Third, any web user has a great number of tools to improve their way of acting online and protect their privacy. To do so, one can keep several advice in mind: personal information should not be inadvertently revealed, cookie notices should be turned on on our Web browser, using instead cookie management software or infomediaries, a "clean" e-mail address should always be kept, personal details should never be revealed to strangers or just-met "friends", highly personal e-mail should not be sent to mailing lists and sensitive files be kept on our home computer as we may be monitored at work, sites that offer some sort of reward or prize in exchange for our contact information or other personal details should alert us, spammers should not be replied to, for any reason, privacy policies and seals should be examined and eventually encryption should be used, as much as possible.

Finally, those major groups are facing increasing brand and reputational challenges. Google for example is frequently regarded as overly-ambitious, entering many new industries simultaneously, often as a disruptor to existing brands and businesses. Google has also been accused of putting the interests of the firm before those of the users. Apple's CEO, Tim Cook has publicly stated that Google systematically exploits personal information to target and serve ads, drawing battle lines over increasing concerns on personal privacy in the digital age. This notion has also been the subject of parody in pop culture.

Perhaps one of the most visible manifestations of Google's reputational challenges was seen on the streets of San Francisco last year, when protesters blocked the company's shuttle buses. For many Bay Area residents, Google had become a symbol of a growing list of problems and frustrations they faced - from high rent to city traffic congestion. But more critically, these protests became a metaphor for an increasing list of challenges the company faces around the world, from tax and government surveillance to privacy and competition.

Google has recently come under some stern criticism, with lawsuits filed against the search giant and anti-Google media becoming more frequently visible. For some people, the searches of Google and the likes of Facebook are indeed trying to reduce our individuality and uniqueness by gradually turning users into more manageable demographic groups (even

though targeting groups by their demographic profiles is not a new trend, as evidenced by the fact that television adverts for food stores inevitably used to air during cooking shows and car showrooms publish their latest offers in motor magazines). As marketers now have the option to target wider audiences who are even more likely to purchase their products or services more directly, it is argued that Google (and Facebook) are building information databases on almost everyone and in doing so, are storing as much information about internet users as they can. Privacy activists feel aggrieved that their browsing habits are being monitored (at least supposedly), whereas the aim from Google's point of view is essentially "the more we know about them, the more we can give to them that we know they need".



We are currently dealing with an increasing number of information that are exchanged between individuals across the world. While a lot of information is given voluntarily (I sign in Facebook and accept the rules), we tend not to be always aware of the information external actors such as government or companies hold on us. Staying completely passive could be extremely dangerous for individuals as they would only rely on those major firms good will. Hence the various legal, citizen and personal actions that have been done to ensure a trustworthiness in anyone's privacy. If this situation holds for the next few years, how will it evolve in the next decades? Where will we be standing in 2050? Will "Privacy" on the Internet still mean something for our children?

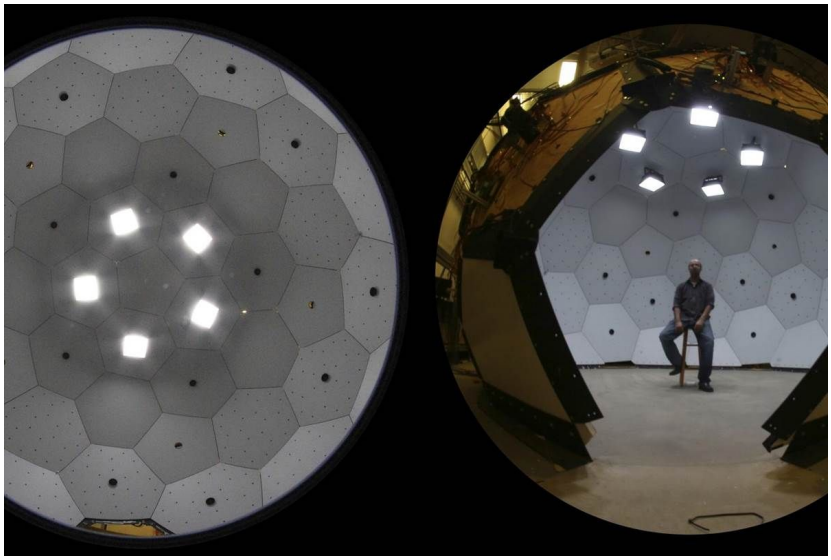
III. Where will we be standing in the next 5, 10, 20 years? Will “online privacy” ever mean anything in the next decades?

“I want everybody here to be careful about what you post on Facebook, because in the YouTube age, whatever you do, it will be pulled up again later somewhere in your life”. Barack Obama used this exact words to express himself seven years ago. Was the US President right? Will Internet soon become more important than your CV?

In 2015, a European court sided with a man attempting to have links to a negative story about him removed from the online search engine Google. Invoking a version of what's known as the "right to be forgotten", the European Union Court of Justice said that citizens have the right to ask that links be removed if they contain information that is "inadequate, irrelevant or no longer relevant". Indeed, the existing rules are confusing, with different legal jurisdictions claiming their (often contradictory) laws all apply at the same time. Besides, much of the existing set of data protection rules was drawn up in the nineties, before the current trend for social networking and high-speed internet had taken off. But this decision has the merit of strengthening individual rights by clarifying exactly what rights an individual has with regards to the data they have personally uploaded (and not at all with regards to the information they disagree with). But will this be globally approved in the future?

To answer this question, we have decided to understand current and future market strategies in two precise industries: social media (Facebook) and online porn.

At Facebook’s 2016 developer conference, CEO Mark Zuckerberg outlined audacious goals for the social network’s next decade. In order to keep the more than 1 billion people that use Facebook every day engaged, and lure in still more users, Facebook has decided to allow companies to build automated “bots” (users can interact with to do things). The firm will also include many more live videos (users comment on them 10 times more than on regular ones) and make it possible to recognize just about anything inside photos and videos. Researcher Yaser Sheikh, a recent hire from Carnegie Mellon University, recently said “Facebook wants to make getting together in virtual space, to catch up with a friend in another city or for a job interview, close to real life”; he mentioned a dome studded with over 500 cameras (named the “Panoptic Studio”, cf. below) to study people’s body language in 3-D as they interact.



In recent years Facebook has rolled out a series of projects aimed at getting more people online. It has provided subsidized Internet access to certain services in dozens of countries around the world and is currently working on a solar-powered drone called Aquila with the wingspan of an airliner to beam Internet to rural areas where cellular infrastructure is too pricey to build. What is more, Facebook has unveiled two new projects aimed at upgrading the Internet: one is a system that uses high-speed wireless technology to wire urban areas with Internet access, as an alternative to laying new fiber-optic cables; another is a way to pack more data into wireless connections used to link cell towers back to their operators and the Web. Of note, Facebook intends to give away the designs for this new technology for free, in the hope that telecommunications companies will adopt it.

Porn companies seem to think the future of their industry lies in interactive, virtual entertainment. An increasing number of US firms have already started regularly producing content for Virtual Reality headsets, which allows viewers to see the films from the performers' perspective and independently look around 360-degrees. Porn firm CamSoda has even started its first live virtual experience, which hopes to transport porn fans into a room full of adult actresses in real-time. Its President, Daron Lundeen, declared in that sense "The adult entertainment industry has long been an early adopter of cutting edge technology and virtual reality is no different. It is quickly becoming one of the most talked about subjects within the industry for its potential to provide users with a truly immersive and transformative experience". Some analysts have even predicted that VR porn is set to become a huge business with $1 billion spent on this new form of adult content by 2020.

What do those two examples tell us about our future online behaviour? We believe that our current fear about protecting private information will help us become more responsible in the

future years. Huge progress have already been made since the creation of the major web actors (GAFA or NATU). Legislation will have to be able to keep up with the innovation of this sector to make sure that privacy remains a fundamental right. But what kind of privacy are we talking about?

We (You) live in a society where you are being told since your childhood that you are unique. Everything is used to make you keep that idea in mind during your entire life. “You must have a personal signature; you must give your fingerprints when you arrive in a new country; don’t let too much personal information on your Facebook account etc”. While this logic is totally understandable, we think that the notion of singularity among a group of people might have come to an end or at least, a change. The concept of privacy will probably evolve in the future decades. You will give more information to your browser, smartphones, social networks accounts on the way you think, the way you act or the way you live. This data will be monetized by major actors playing in the new technology sector. They will know what you do and what you did 15 years ago. They will even be capable of anticipating what you will be doing in the coming hours, months… Actually, we will all be in that situation. The growing number of users linked with the exploding number of data will force those companies to sort the information. They simply won’t be able to store that data forever. What could they still learn from consumers purchasing behaviours on their website 2 years after their last purchase for example? What does a search made 32 years ago by a man tell about him?

We believe that the future prospects and evolutions of the Internet use by worldwide consumers will lead to an auto-destruction of data. Hence an online privacy that will be held for a time period of 2-3 years maximum as your information will always be of less value as time goes by. The privacy on the Internet will remain a sweet dream and people will still have to be careful about their online behaviour as their data might be reused later on (more particularly the “naked” kind of pictures). Still, all your other information (where you have been, which photo you have liked, which website you have been surfing on) will naturally disappear with time. Unless you disappear before… And then, what happens to all the content you have created, your online accounts and virtual transactions? What happens to all the things you have stored in the cloud and, unknowingly, in servers across the globe? There is no single answer to these questions. However, if there is one lesson to be drawn out of all these reasonings, it is certainly that with the redefinition of the privacy concept due to all the evolutions of the Internet, most of us definitely live two lives, a physical one and a virtual mirror of it online. And when we die, our physical existence will come to an end even if our virtual presence will linger on. A sarcastic way of rephrasing Orwell’s quote in our virtual but humanly time-limited world could consequently be: “*Dig Brother is watching you*”.

Bibliography

- *The Magazine of UC Riverside, Fall 2013, The changing face of privacy*
- Rosen, Jeff (2010), *The Web means the end of forgetting*
- Eggers, Dave (2010), *The Circle*
- Buchanan, Tom and co (2006), *Internet users' perceptions of 'privacy concerns' and 'privacy actions'*
- *https://blog.kissmetrics.com/guide-to-reputation-management/*
- *http://trends.ifla.org/expert-meeting-summary/the-future-of-online-privacy-and-the-security-of-personal-data*
- *https://medium.com/the-ferenstein-wire/the-birth-and-death-of-privacy-3-000-years-of-history-in-50-images-614c26059e#.e9clm7gqh*
- *http://www.forbes.com/sites/larrymagid/2013/02/12/online-privacy-and-security-is-a-shared-responsibility-government-industry-and-you/#1d537b243439*
- *https://www.theguardian.com/technology/video/2015/jul/09/virtual-reality-future-porn-video*