



Università degli Studi di Trento

Privacy and Digital Technologies: E-Dossier

Joseph Brian Musanje Kasozi

166047

Submitted to :

Professor Rossato Andrea,

Professor Vincenzo D' Andrea

June, 2014

Table of Contents

Executive Summary	3
Introduction.....	4
Background of privacy and digital technology.....	5
The Rise of Electronic Dossier and the fall of Privacy.....	5
How Data is collected	6
E-Dossier at Google.....	7
Google Privacy policy	9
Who controls the Electronic Dossier	10
Conclusion.....	12
References	13

Executive Summary

Privacy has been a key issue that needs to be addressed in the digital era. With development of digital technologies now information is shared so easily and fast. The rise of online giants like Google who collect personal information has also affected the privacy even more. This paper shows how privacy was conceived before the digital technology and how its conceived today in the digital era where every online user has a clone of him or her stored on a server. This clone will be referred to as an Electronic dossier throughout this paper. Privacy laws were put in place to see that privacy can be maintained even when using digital technologies but this hasn't been enough and therefore the paper suggests some more alternatives than can be done by user in order to keep their privacy right.

The world is never going to be perfect,

either on- or offline;

so let's not set impossibly high

Standards for online

-ESTHER DYSON

Introduction

In today's world, we are using digital technology in ways we never imagined were possible. People are "plugged in", connected through a variety of tools that is to say mobile devices, computers and applications for example social media platforms and blogs. Now information and people are more accessible than ever before. In the past a few years we have experienced a drastic transformation in social, economic and political being. Small information that was stored in paper files or small papers which would fade and rot away is now stored in computer memory forever. People use ATM, bus cards, credit cards, no one moves with physical money. But all these cards can be used to track what we do, where we are and what we earn or spend. Every second that passes, gigabytes of information stream into electric brains to be sorted and rearranged into a number of different ways. Digital technology enables the preservation of our daily comings and goings including our likes or dislikes, which we are, what we do, where we go, what we own. One's life is captured in electronic records and hence creating an electronic crone of an individual. This has lead to what can be referred to as "Electronic Dossier".

According to the Oxford dictionary a dossier is a collection of about a particular person, event or subject. These were or even are currently used in European courts to assemble information about a person in order to reach a judgment [1]. Incidentally with the digital technology dossiers are created on everyone who has uses digital technology. Data is changed into binary format which is stored and manipulated using computers. Here keeping all one's personal details in huge databases created by multi companies all around the world in the name of social networks, E-commerce and other technological advancements in this technological era. Where is this data going and what happens next?

Privacy has been a critical social issue associated with digital or information technology for as long as these technologies have been in existence.

Privacy is conceived in different ways depending on the territory or location but Privacy can be defined as one's life but with exclusion from publicity [14]. The concept follows from the right to be left alone [12] [13]. Shank (1986, p. 13) states that such a perception of privacy set the course for passing of privacy laws in the United States for the ninety years that followed. Therefore privacy is considered a natural right on which the legal rights are based. It's therefore noted that privacy is protected by the private law while in Europe there is no statutory definition

of privacy rather privacy is considered to be in the shadow of law. It is also as the right of personality. Privacy is intended to protect an individual from social projections [10].

Background of privacy and digital technology

Data or information privacy has been a main concern in the digital technology era. Many laws have been set concerning privacy namely common law torts, criminal law, law of oblivion and many other statutes around the world. But the question is how did privacy come about? Let answer the question by taking a brief background study of the privacy right. The emergence of privacy has been greatly impacted by technology and in response many new statutes and laws have emerged. These laws are as result of the ever changing technology that has increased the use of personal data. [2]

The relationship between the legal issues, public expectation of privacy technology, use and collection data is what is known as information privacy. [2]

Privacy can also been seen as part of one's possession of facts of his or her life from simple text or digits to like and dislikes [10]

In the early day privacy was commonly related to surveillance but then later in the 1960s companies started collecting individual information and storing it in databases. This was a clear violation of one's privacy right and people also feared the occurrence of data shadows

The Rise of Electronic Dossier and the fall of Privacy

There exist many companies working on capturing and storing peoples personal data for both security and business reasons. In this study cases studies will be done on the commonly know online companies and organizations today which focus their main business processes on the personal data collected from individuals. This data collected and stored forms what is termed as the electronic dossier since an individual can be tracked and identified from the rest by using this information. Google being one of the biggest online companies, it will be used as a case study to demonstrate the rise of e-dossier and fall of privacy in the digital world today.

An electronic dossier is developed on someone from the point of birth mostly those individuals born 20 to 30 years back in time. The hospital captures every detail about the new born baby

that's the name, date of birth weight color, parent's place of birth and much more. From this point data is stored on this baby in digital form using the digital technologies. This data will grow as the baby grows and some is privately kept by some organizations or government agencies and other is public. From the hospital as the baby is growing up pictures are taken and uploaded on social networks all this is mapped to one individual. therefore if this baby now a grown up wants to get a job the employer will search online get all the information about the employee from there the employer is able to judge if or not to give the job .More about the raise of electronic dossier can be seen the case study of Google

How Data is collected

The dossier has rose from a number of technological activities and each has an impact on the privacy of an individual and these include the following common acts

Massive Surveillance Systems

The system was originally set up during the Cold War but it was not confirmed until a few years ago when secret documents of the National Security Agency, NSA, were declassified [4].The system intercepts and gathers daily communication including phone calls, Internet downloads, email, satellite transmissions and much more. Then the information is sorted and refined through programs using artificial intelligence

The techniques used for this kind of massive surveillance could be used to violate privacy even more in the future. Imagine what the result would be if a similar system was developed but instead of gathering the Internet communication it collects personal information from computerized databases and correlate the information to a specific person. It would definitely be the end of what we call privacy today.

Online Forms and Social Media

It's worth mentioning with the current social platforms where people are free to post share information. Most social media are not even aware that they are creating their own dossiers while providing information. This information is captured and stored in digital databases. A good example of privacy violation is with Google plus Social Platform managed by Google. At the beginning of the year 2014 in January Google plus produced a short video for each and every user who has an account. On Google plus one is able to have private pictures which are not accessible on the public profile. But it was noted that this generated video comprised of only pictures that are auto backup through one's mobile device which are supposed to be private.

While having a Google account one can never delete information provided apart from updating it thereby updating one's electronic dossier.

Banks and Electronic Commerce

When one opens up a bank account in any bank regardless of the region or territory his or her personal information will be captured and stored in the bank's digital databases and later the client is given either an ATM card or even credit card. These cards are a unique identifier of this individual. One is able to perform online transactions and his financial information is captured by both the bank and the E Commerce companies there by building more on his dossier

Government institution or Public Institutions

These capture information of all the citizens in the country and this information is stored electronically. This is an addition to ones electronic dossier. These include universities, schools, hospitals, Police and many others. All these capture different information about the different categories of people and hence contributing to the electronic dossier

Case Study: Google

Google is an American multinational corporation specializing in Internet-related services and products. These include online advertising technologies, search, cloud computing, and software [8]. Most of its profits are derived from Ad Words. Google provides free internet services including Google search engine, Google News, YouTube, Google blogs, Google plus, Google maps, Gmail, Mobile platform, Google drive, Google calendar, Google Keep, Chrome, scholar, Cloud Computing and Code Platform. One is able to access and use all these service for free. The only constraint for one to use any of the services is that one should have a Google Account. To set up an account one's information will be captured and stored by Google. This in include: Names, Phone number, Location, Date of birth, Previous or current email and a picture. After this information is captured and stored one is granted a free Gmail account. Now with this email account you are able to use any of the Google free service

E-Dossier at Google

When setting up a Google account the basic information of an individual is captured and this include the name address and contact after which a unique email address is mapped to the personal data .Now an individual is uniquely identified by the email address. This email address is used when accessing the all the other free Google services.

How does this create a E-Dossier

An email is mapped to one individual, therefore when you access other Google services with your email then Google will always keep track of what you are doing hence creating a big set of data about an individual.

Starting from the email Google will keep track of whom do you send email to, when do you send email, how many emails do you send? Through the email address Google is also able to keep track of the device you are using by its MAC address or even the processor number. Next are the Google maps. When using Google maps on a mobile device Google is able to use the GPS to track where you go every minute. Therefore Google keeps track of the restaurants you visit, the Hotels you visit during a vacation; this information is also added to the basic information captured with the email. On addition when using Google chrome and saving bookmarks, these are stored remotely on a Google server so Google is still able to know what sites you visit often. This can also be done by use of cookies. Google can also store more data on an individual through the Google Search engine, here they capture and store all the searches one makes with the engine. So if you are planning to go for a holiday and you search for best hotels, or flight deals, all this information is stored in Google's servers.

This company earns most of its income from adverts therefore it will use this information provided by the user to provide relevant adverts to the users. Next time when one is searching for a hotel, Google will just retrieve the location and return the hotels near your location or if you are searching for a restaurant, Google still will provide ads for nearby restaurants. Lastly with Google play, one can buy applications .when buying an application you use either PayPal, Google wallet which are all mapped to your credit card. So by buying an application Google is able to know the money you have on your credit card.

Therefore here we see that Google now knows where you are , what you want, where you stay, what you like watching, where you like to go, what airplane you use to travel, where you spend your holidays, how much money you have, how you spend your money. In other words Google has a clone of you and hence no privacy at all since every detail of yours is known to Google and you have no control over your data you provide since even most of the time someone doesn't know that his data is being captured and stored remotely somewhere in a server.

With all the Google services we see the rise of an electronic dossier. One's data is being captured and stored and who knows? This data can be used against him or her just like the dossier used in the European courts of law.

Google Privacy policy

This privacy policy was last updated on March 31, 2014 and it comes with more changes. It comprises of [9]

1. What information Google collects and why they collect it
2. How they use the information
3. The choices they offer , including how to access and update information

What information is collected by Google

Information is collected in two kinds of ways [9].

- Information provided by the users

This information is provided by the users for example when setting up a Google account some personal information is collected

- Information captured from the use of Google services

This information is collected depending on the service used. For example when one interacts with the Google ads or using Google maps, someone's location is stored in the process. Information collected in this form includes Location, log information, telephony log information, local storage information, unique application numbers and device information.

How data is used

The information collected is used on the Public Google profiles of the users and also other information like emails are used for communication .More information is combined with all information collected from the different Google services to make it easy for users to share any information they are willing to share .

Google policy and user privacy

Having reviewed the Google privacy policy, the level at which users control or manage their data is to low. Google owns all the control of this information although the user through the Google dashboard is able to edit and update their information. But this does not provide the user to delete the information in case he or she wanted to remove any details from Google. But the Google privacy explains that Google will use and share some personal information with other companies

or organizations and this is done without the user's consent [9] thereby infringing the user's privacy.

In conclusion Google does not give users enough control over the data it collects about them. This data is used to create a digital personality of an individual but the individual with whom the data is collected has less or no control over it.

Who controls the Electronic Dossier

A dossier in traditional view is controlled and managed by the courts of law. The individual with whom the data is collected has no control over what kind of data is being collected about him. Likewise the electronic dossier created on every individual. The people whose data is collected have no power over the data they provide. The organization that collects the information or data has full control over the data collected.

Electronic Dossier versus Privacy

Comparing an electronic dossier is like comparing revenue to privacy. This is because most of the collected data today is mainly for marketing and hence creating revenue for the company in question. But on the side of the data owner his or her privacy will be declined since his information is being shared all around the web and maybe he would like it to be private.

At the level of an individual, the violation of privacy effect is considered as infringement of one's dignity as well as limitation to freedom. In Rosenberg 1994 research she concluded that "Technology continues to be viewed as a threat to privacy rather than a possible solution" as surely this is seen in the current state of technology. Privacy is being violated more and more than finding a solution to control the infringements.

Economically and socially this comes with a positive effect now that there is growth of large businesses like Google and telecommunication companies who get their main income from trading off people's personal data and hence growth in the economy but also it now opens up the mind of the legislative body that there is a need to protect privacy.

Although the electronic dossier has a negative impact on privacy on the other hand one's electronic dossier can help you find things you really want, it can help companies provide better service, and perhaps in the future the world-wide-web will be tailored to fit you. This can be seen with Google on how to keep on improving its services to fit the needs of the clients or users.

Recommendations towards the improvement of Privacy with digital Technologies

The current law to privacy has solved a number of challenges although it has still faced a number of failures and difficulties in solving the privacy problem in the digital world. But why has the law failed to perform effectively and how better can we make the law work in the ever changing digital world. Always there is a development of new technology which has effect of privacy. Protection of privacy is a human right and one of the foundations of society where individuals safely can enjoy the freedom of speech. The functionality within the digital technologies depends on the individuals' capability to use the technology without worrying about having their personal information gathered in a database and later on becoming a victim for example spamming and identity theft.

Legislation can work but as noted in the current state it has not solved the privacy problem. Still people are providing information both voluntary and involuntary then this information is shared and accessed by big companies to which an individual wouldn't be able to sue in the courts of law.

Therefore on addition to legislation or law. There some more suggestions they would help individuals to preserve privacy in the digital world and these include;

Always individuals should be aware when providing personal information, before one provides personal information to any system or site, he should be notified about the privacy the site provides on addition to as to why they need the personal information and how much control does one have over his information. By doing this one will provide information already knowing the consequences so incase the information is made public and this person was notified during the collection process, it will mean that no privacy problem has been caused since the information owner knew that his information will be made public.

User should not reveal personal information to strangers, Spammers are a good example of strangers, In order to protect your privacy always ensure that you don't share your information with strangers be it on the social networks , emails or any other digital technology.

User should keep a clean email; by this a user is able to only provide his contact to trusted companies or users. In case you are publishing a web page with your email make sure you only publish an email that won't affect your personal image and privacy. In case you use the same

email in other critical services this wouldn't be advisable to share the same email with the rest of the online community

Always users should manage their web browsers. It is advised to always disable cookies in web browsers while surfing the internet and working on critical personal information. With cookies disabled the browser is not able to send out any personal information without a user's consent unlike when they are enabled. Here the user will be able to keep his or her privacy even without the legislation building up laws.

Other ways in which privacy in the digital era can be reached is by the following key notes.

- Users should be aware of sites that award prizes in return to information
- Be conscious about web security
- Use encryptions while send messages over the internet
- Disable Global positioning system on the device when it's not required
- Before using any digital service or technology examine the privacy policies and seals

Conclusion

The age of information distribution has arrived and regardless of the varying opinions concerning social networking sites, online technologies and the entire digital technology terminology it is important that individuals are aware of the risks as well as the benefits that these services may inadvertently provide. In the present situation, regardless of whether someone posted the information or it simply exists in cyberspace, protecting oneself is a serious concern therefore everyone should take action towards the protection of privacy.

References

- [1] <http://www.oxforddictionaries.com/>
- [2] https://en.wikipedia.org/wiki/Information_privacy
- [3] http://www.nnedv.org/docs/SafetyNet/OVW/NNEDV_HighTechStalking_Tipsheet_2010.pdf
- [4] BBC, "US spy system under attack" (February 23, 2000) news.bbc.co.uk/1/hi/world/654394.stm - 2014-05-09
- [5] Simson Garfinkel, "Database Nation – The Death of Privacy in the 21st Century", O'Reilly (2001)
- [6] Bruce Schneier, "Secrets & Lies – Digital Security in a Networked World", John Wiley & Sons (2000)
- [7] Matt Richtel, "Rampant Trade of Stolen Credit-Card Numbers Shows Lack of Security" (May 12, 2002) www.siliconvalley.com/mld/siliconvalley/news/editorial/3252532.htm?template=contentModules/printstory.jsp – 2014-05-11
- [8] https://en.wikipedia.org/wiki/Google#cite_note-See:_List_of_Google_products-6
- [9] <http://www.google.com/policies/privacy/>
- [10] <http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm>
- [11] The magazine <http://hbr.org/2008/10/what-was-privacy/ar/1> (2008)
- [12] Stair, R.M. (1992). Principles of Information Systems. A Managerial Approach. Boston: Boyd & Fraser, pp.635,
- [13] Shank, R. (1986, Summer). Privacy: History, legal, social, and ethical aspects. *Library Trends*, pp. 7-15.
- [14] Neethling, J., Potgieter, J.M. & Visser, P.J. 1996. *Neethling's law of personality*. Durban: Butterworths, pp 36
- [15] <http://web.simmons.edu/~chen/nit/NIT'96/96-025-Britz.html>