Internet & Privacy

07209525 - Benjamin Goupil
benjamin.goupil@gmail.com
MsC Multimedia Computing
CS4S17 – Independent Study

Summary

1 - Abstract

This paper is concerning Internet and the privacy. This paper will try to cover a maximum where are the threat about privacy.

It begin by defining what is privacy and it context in computing, then, it will explain main threats and consequences of private information in a public place. In fact, what people don't want to see and experience. After, what privacy is behind main services used by people on Internet, understanding technologies help the user to determine the line between public and private information.

There is a guide to protect yourself. In fact, it's hard to establish a fine guideline. The principle here, is mainly understanding concept and the way to define private data independently to the service (Facebook, Google, etc...).

2 - Introduction, what is privacy ?

In France, we talk about «right to intimacy and privacy» and this notion is included in many principles in the law (Serge Braudo, 2009). The constituents of the private life were not the object of a definition or a restrictive enumeration to avoid limiting the protection to the only legal forecasts. The courts applied the principle of this protection, in the right to sentimental life, in the family life, in the secret concerning the health, the residence, and concerning the right for image (How a person is view trough media). So privacy is all activities of a person which concern his intimacy opposite to the public life. The right to privacy is in the constitution (In France). The limit between public and private life is subjective and specific to each culture, country and person. Then, privacy is conceptual and variable in places and over time. The control of this privacy is the ability to select what can be reveal or not.

On Internet, privacy is concerning what users let on website as personal informations, as data voluntary given to the website (like your name on Facebook), as data manipulate by your web browser (cookies,...), as data manipulates by the network itself (Like the Internet Protocol (IP) address given by your Internet Service Provider (ISP)). All these elements have not the same value as personal information and are not considered as personal information is all countries, like the IP address for example. Private information can be online by indirect way too. Your house can be easily viewable with Google maps for example or friends can identified you on Facebook or in general, social networking website. Also, it can be from your Operating System (OS) during an update or it registration/activation (Other software are concerned too).

So, the area of privacy linked to Internet is wide and not easy to control.

3 - Internet, the new Big Brother ? Consequences...

Control privacy things in the real life is easier than on Internet. Because Internet and computing in general is not well use and understanding by common people, because people don't know what, when, why, for what... data are sent and because they don't have consciousness about what they do on Internet (Except a little part of the population like geeks who try to understand how it works).

3.1 - Jobs

One of the main problem when someone provide private informations on Internet is how that can influence the future of this professional life. In fact, it's the most dangerous case with a long time view. In a study publish by Microsoft for the «privacy day» the 28th of january 2010 (Cross-tab for Microsoft, 2010), 70% of american recruiters, 41% of english, 16% of german and 14% of french have rejected a candidate due to what they have found on him on Internet.

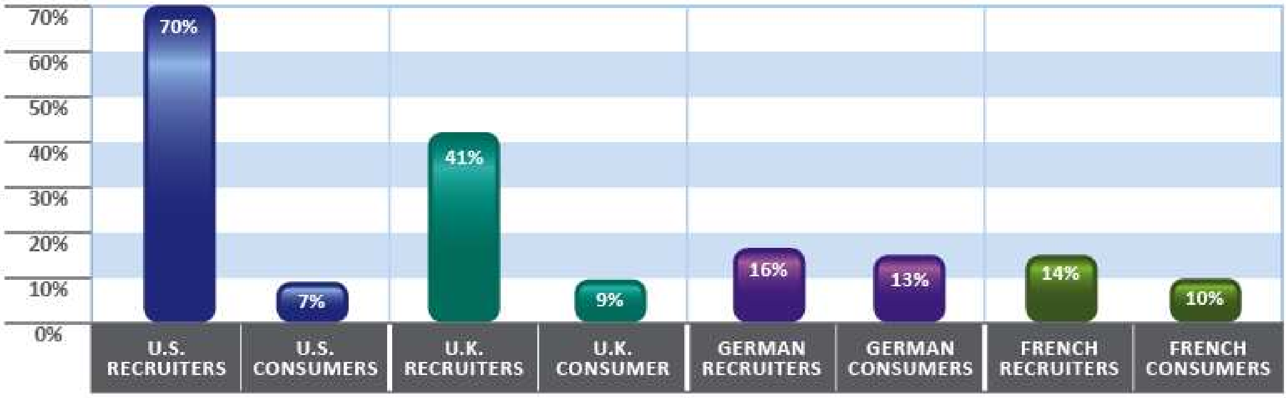
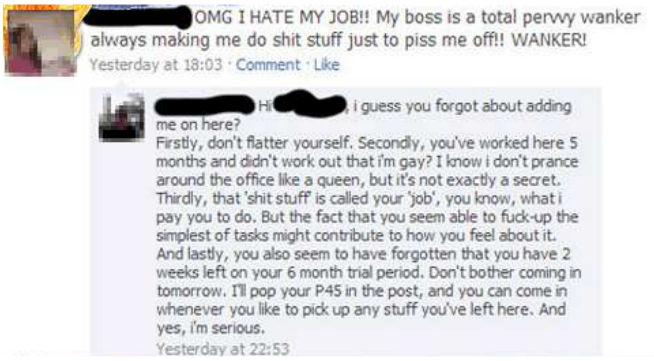


Illustration 1: Recruiters and HR professionals who have rejected candidates based on data found online versus consumers who think online data affected their job search.

If we doesn't know what is the interest for recruiters, there motivations, when they grab data on a candidate, we don't know how many candidates who have apply for a job have been employed with regards to what they have put on Internet as personal informations.



[redacted] OMG I HATE MY JOB!! My boss is a total pervy wanker always making me do shit stuff just to piss me off!! WANKER!

Yesterday at 18:03 · Comment · Like

[redacted] Hi [redacted], i guess you forgot about adding me on here?

Firstly, don't flatter yourself. Secondly, you've worked here 5 months and didn't work out that i'm gay? I know i don't prance around the office like a queen, but it's not exactly a secret. Thirdly, that 'shit stuff' is called your 'job', you know, what i pay you to do. But the fact that you seem able to fuck-up the simplest of tasks might contribute to how you feel about it. And lastly, you also seem to have forgotten that you have 2 weeks left on your 6 month trial period. Don't bother coming in tomorrow. I'll pop your P45 in the post, and you can come in whenever you like to pick up any stuff you've left here. And yes, i'm serious.

Yesterday at 22:53

Illustration 2: An example of what don't be done ! (from http://failbooking.com/2009/12/28/funny-facebook-can-she-still-get-unemployment/)

There are many examples in the world about people who have been fired due to their online activities. Mainly, informations have been found on social networking websites. People add their colleagues and their boss on Facebook, publish private things or particular opinion and can have problems. They forgot that Facebook is a public place.

A trainee in a bank have argue that he have family problem, so he have sent an e-mail requesting the authorization to not working the day after. But, a person have found on Facebook a photography of him during the last night party... He have been fired.

A job seeker have a surprised when a human resources individual have give him a picture presenting his “buttocks” found on Facebook. It was one of the first result in Google (RTL Info, 2009).

An international finance lawyer, Deidre Dare, who works for Allen & Overy, in Moscow, has some problem with her bosses since they have found pornographic story (Casey Lynn, 2010)(about the life of a fictional firm in Moscow) and erotic picture of her in underwear. Casey Lynn says about this story: “*One of the first things they have done is to tell first year law students to check your Facebook page and make sure that you don’t have any pictures posted of yourself doing keg stands during Spring Break or have your favorite movie listed as The Cannabis Grow Bible. It might not be fair, but the truth is, if you’re going to work in a certain job, especially if it’s high-profile, then you’ve got to keep your public face clean.*” The lawyer have to stop to write next chapters, existing chapters can be downloaded like photography.

There is also an example with Twitter, which is public by default. @theconnor: “Cisco just offered me a job! Now I have to weigh the utility of a fatty paycheck against the daily commute to San Jose and hating the work.”. Response from Tim Levad, Cisco: “Who is the hiring manager. I’m sure they would love to know that you will hate the work. We here at Cisco are versed in the web.”. The result of this comment is not know even if rumors said she not have been hired.

For a group of french recruiters, there is an ethical problem to use personal informations. So, a group of 40 firms specialized in recruitment have decided to only use professional networking Internet websites like LinkedIn or Viadeo and not Facebook to give a chance to everyone to have a job and not take in consideration subjective elements we can found in private life. I think, that's needed in order to don't see technologies like a trojan in our life and use them with a lightly spirit.

3.2 - Teenagers

When we see how people, especially teenagers, are exposed on the web, we can think that can have many repercussion on their life later. One of the problem is about what type of problems they can have if their boss can access private informations like photography during a party, politics opinion,... This think is exactly the reverse of the previous generation which thinking that privacy must be protected and not exposed everywhere.

Jean Marc Manach is talking about the relation between teenagers and privacy on Internet in an article called « Vie privée: le point de vue des « petits cons » ». On this article, he is explaining that teenagers are looking privacy in another way that people. They know there is risk to be expose on Internet but they are aware and data are share with control, even if data shared appears to be really personal.

With the new trends of the web, especially the « Web 2.0 », we can view users provide many information about their life. We can think that they are not aware about privacy and risks but it appears that teenagers view is the same as their parents due to generation differences. For Jean-Marc Manach, there is the same difference between teenager now with their parents than their parents during the sixties and the sexual revolution, which appears to be something exceptional for their parents too. So teenagers apply on Internet the same liberty as their parents have acquire with success in the real life previously. Danah Boyd add teenagers need a free space without parental control and argue that they don't have in real life a really private space, bedroom can be locked but parents can go in when they want. For example, they can discuss trough portable phone (with SMS) or on Internet trough forum and instant messaging without this aspect and anonymously if they want, that is liberty (for them).

The point of view of privacy is different and that can be rude to understand for parents. They need to talk to their child about privacy and consequences before child subscribes to a service.

3.3 - Education of Internet

Children and teenager have now an easy access to Internet at home. Previously, Internet was accessible only at school, where computers where accessible too. At school, the network is organized to protect children against a lot's of bad effect (Fabrice Prigent, 2010) of the web: pornography, violence,... and is considered as a fantastic tool for education.

At home, there is no specialist of computers and Internet so it's difficult for parents to maintain a secured access to it. Plus, now, game console can access the web (and that will be probably a standard feature on game console and way to go to Internet in the future).

The main risk with children on Internet is chatting with webcam to an unknown person. Problems are linked to pedophile: from nudity in from of the webcam to sexual violence in real life.

Computers and Internet must be understanding a little by parents to control what their child doing on it. ISP help parents by providing some software which allow them to control access websites or services filtering and categorize by risks: adult, agressif, dangerous-material, drogue, gambling, phishing, warez, filehosting, sect, malware, chat,...

Risks can come from a wide area of subject (Sébastien Sauvage, 2010) but protection is not the only way to protect and really not an advantage with a long time view (and not only concerning privacy, but also security in general on Internet). Children have to learn and experience Internet (Dimitri T., 2010). It like learn how to use a bicycle or drive a car, the more you use Internet, the more you easily identify threats and reduce risks for you or you computer. Remember that if parents are not agree with the limit fixed by their child, it's because they don't have the same honor/value system.

4 - Technologies

4.1 - Instant messaging

Instant messaging is, why navigation on the Web, the main activity for teenagers on a computer. One of the main tool used is Windows Live Messager. Due to the popularity of this protocol and software, many traps have been created like clicking on a dangerous link sent by a friend (his/her computer is infected by a virus). Then, there are risks to met the wrong person who try to convince young boys and girls to be nude in front of their webcam. So it's dangerous and must be controlled by parents.

More about privacy, the MSN protocol used is “in clear text” on Internet and your home network. Messages can be intercept using a man in the middle attack join to a software like Wireshark to read , in real time, packets of data, it's not protected with an encrypted tunnel layer like SSH. Plus, MSN is a centralized instant messaging protocol. All your data pass trough Microsoft's servers and filters. Microsoft doesn't send messages with special keywords (http://[address]/download.php, http://[address].pif, http://[address].ath.cx,...) or file shared with certain extension (exe, bat, js, hlp, chm, msi,...). This censorship is probably server-side. With free and open-source software (like Emesene or Pidgin), the result is the same. Microsoft announce that is for the security of the MSN network and protect users against threat from Internet.

4.2 - Spyweb

Spywebs are all threats which have for origins non legal software, hacked software (with a crack executable for example) and website which use badly your information but without say it to you (That not concern Facebook for example, Facebook communicate how it use your personal information).

To be clearer, put “VLC” in Google. VLC is a software multimedia player which run on Windows, Linux and Mac OSX. It's a free and open source software. The first result is a commercial link on a non-official website. The file downloaded is not the official file, plus, when I run it, it demand if I want to make Puc**.com as welcome page in my browser and as default web search engine. The test was stopped here, the risk is high to install a crapware, plus, the executable file have been executed...

VLC is not responsible of that. Some people want money and act without respect for the original software. Ccleaner, another software, was in the same case but now, many months after, Google is clean up. With Ccleaner copy, you have to paid to run the software...

To know how your software communicate with Internet, it's necessary to install a firewall, which prevent from unauthorized access from Internet to your PC and vice-versa. And try to download files from well-known and secure sources.

The main problem with spywebs, is not really fake software, it's more fake website. Definition from Wikipedia in English: “*In the field of computer security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Even when using server authentication, it may require tremendous skill to detect that the website is fake. Phishing is an example of social engineering techniques used to fool users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures.*”

This is one of the most important threat now on Internet. Phishing try to grab your data from bank, insurance, ISP, social networking websites. By verifying the link where the software or website wants you to go, you probably avoid the risk. It can be done with several manners. In a web browser, by activate the status bar. The status bar allow you to watch where the link goes. Also, you have to verify the address of the website, even if the address looks identical. For example, www.whitehouse.gov (official) is not the same as www.whitehouse.org or www.whitehouse.com. That is called cybersquatting.

4.3 - Google

Google offer a nice collection of useful services and software. But Google know what you are looking for, visiting or reading with it research motor, globally, for the connected population (Google see trends) but also on you if you are connected to your Google account (Gmail for example). It know what you will doing with Google Calendar and because it's linked with Gmail, perhaps what person and for what reason.

It also know what are your centers of interest with Google Adsence (if you have click or not on a link, because it's the main advertisement system in the world to make money) and Analytics if you have your own website. And it's popularity with the rank of your website, a mark on 10, plus what is doing your firm by analyzing words you have buy. If you use Google Docs and/or Google Desktop, it know what you do in details including the subject of your meeting you have planed previously. It know what is the part of type of document on your hard drive disk even if they are confidential, what software you use by analyzing the program installed folder (like some other intrusive software like printers driver. The argument is that the program scan to find software to associate with pictures editing and organizing...). It know a lot's of precise things like your home address, your mobile phone number, because it's include in your documents or being use in Google Maps.

Now, Google have it's own mobile phone and mobile operating system. That increase the potential dangerosity of Google because it can know where your are (because smartphone include a Global positioning System (GPS) by default), who are your contact and what is the content of your SMS/MMS. Plus, Google have it's own applications market place (Store) for Android based phones and can do statistics on it too.

4.4 - Facebook

Facebook is probably now the most important social networking website at a world scale. The good things with Facebook is that allow users to retrieve or make contacts, see what friends like or not, share video and photos and play games (in order to compare results with friends). The idea is good and the success is here with approximately 400 millions users in december 2009. Marc Rees from PCInpact.com says that Facebook is now a challenger for Google for the online searching. For CyberSentinel.co.uk, teenagers share their life during 1h40 per week.

For subscribing, you need to provide some basic data like name, surname, date of birth, e-mail address, sex and password. But after, Facebook try to invite you to complete with your city (of birth), your love status, your sexuality orientation, your opinion about politic and religion ! And that is just the first tab, there are also more personal information, localization, school and job things tab to finish. That is a huge mass of information. Facebook can made a profile just with that. The danger is the user itself who provide all data.

The data are acquired with fan pages, when we become a member of a group or by the interaction between users trough your "wall". A personal (as editor) but public place where things can be shared (text or hyperlinks for audio and video files on Youtube for example). Subject can be analyze but links too, perhaps a link with a special video on Youtube can signify something. Plus, can can add comments so the relation between your personality and things on Facebook is easy to analyze.

Facebook try to know more about you when it suggest things to do and when you see friends in a group for example, you can be able to provide personal data involuntary (but it's encouraged involuntary by friends too, you can't change parameters on this functionality).

The risk is multiply by the number of applications which can be provide trough Facebook from firms. And we can't know what is the real process behind applications. Facebook just says that external applications must use personal settings to protect privacy but there is no verification. And data are not stored on Facebook servers, it's a risk because if a hacker have compromised an external server, he can access too this data. We know nothing about who store data and who is responsible in this case. All of that things is explained in the agreement between Facebook and users. But who read that ?

Plus, Facebook have, in February 2009, try to change the policies about confidentiality to allow it to sell, modify, distribute data. And data provided by users will be the property of Facebook. Because of the users implication for don't change policies, Facebook have canceled that, but we can see the spirit of the firm about privacy and the future can be bad.

Rumors says that Facebook will change settings about external partners and make public certain type of data even if you don't use the external service (Marshall Kirkpatrick, Fabrice Epelboin, 2010) (Vincent Hermann, 2010). Be sure to protect your data as you want. Change or delete your Facebook account if your are not satisfied !

5 - Other types of problems

As we have seen previously, problems can appears from a lot's of different things, for example, if you book an hotel room, you'll be asked to give your bank card number (including the cryptogram behind the card) on the hotel's website or by e-mail. But you don't know who is responsible of your data. Your e-mail can be printed and stored in a public (or semi-public) place like the hotel “welcome” desk. And information are store on a computer but you don't know the architecture and the security applied to this server.

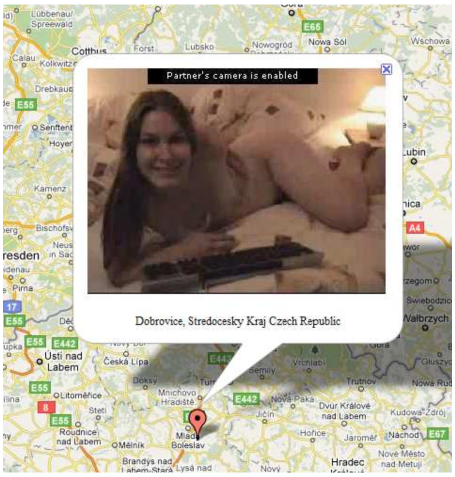

Partner's camera is enabled
Dobrovice, Stredocesky Kraj Czech Republic
Cottbus
Dresden
Ústí nad Labem
Mladá Boleslav
Hradec Králové

Illustration 3: A screenshot from chatroulettemap, the girl can be identified now.

There are new type of websites which have appears recently based on the same idea as the first of this type on Internet: www.chatroulette.com. This website is very special: you allow the website to use the microphone and the webcam built in your notebook, then, you are ready to have a visio-conference plus chat with another user but randomly chosen. If you are not, subjectively, a person interesting for the other, you can be “nexted”. You can “nexted” the person too. The service has been describe as “anonymous”. The problem is, several days after the “buzz” on the Web, a new website has appear, called chatroulettemap, which associate a connected (or previously connected) user to a geographical location, using Google Maps , with their name (not real) and an image from their webcam. So most of them can be identify because we can see the head clearly, and not just the head... You just can call the service after being on chatroulettemap. Plus, many photography are sexually explicit and can attract potentially dangerous people on a “target”.

In your web browser, like Firefox, Opera or Internet Explorer, you can delete your cookies and some others things about your online activities. What is a cookie ? It's a little file which indicate to a website technical or personal things. For example, it can be your screen resolution or the content of a basket on a commercial website. It can be use to identify a user with his preferences. But it can be use by many spywebs, so even if they are not dangerous, they are deleted by security tools on your computer. With flash, it will be possible (but it was impossible for a long time) to delete flash cookies with the 10.1 version of Flash Player. This future version of flash will also respect the private navigation mode include in modern web browser.

Flash is also a technology with several security issue. On each version, researcher in security have discovered important failure which can allow a black hat hacker serious damage. From a crash of the operating system to a remote control with root (administrator) access. When a computer is corrupted, now, by a threat, it's often to steal privacy information, especially credit card number, because it's hard for a main part of the online population to understand where the possibility of a danger exist (and how to be protected).

Technically, some other technologies are concerned, the last is Adobe Reader (Jérôme G., 2010) (Lee Mathews, 2010) and Java. Mozilla Firefox inform the user and allow him to desactivate Java. Everyday there are news like that.

Your secret question can now be found on social network website, and your intimacy revelated (Nil Sanyas, 2010, n°12). Everybody have now to check if your secret answer chosen a long time ago can now be found easily ! That the story of the Twitter hack (Nil Sanyas, 2010, n°14 and 15). And it not concerning users but administrators. But you can found articles about how to improve your safety on Twitter (HiTechno Corner administrator, 2010).

6 - Guide to help to protect yourself

6.1 - In general, define privates information and control them

Privacy, is mainly, what we decide to keep private. That varying from a person to another. But with experience, you can thing that you know the subject and think about it too lightly. In fact, before separate what is private and what is public, it's really important to know if we really needs to provide certain data to a website, especially Facebook, which is changing is terms of services a lot's of time (with many rumors about privacy threat). So you can't be sure that your privacy level will be the same all over the time, and well controlled by yourself. Try to provide the minimum as possible personal information. Looking settings and change them can improve privacy to not allow all people or firm when they are looking your public profile, the ads tab will be really important for the future, you can say “nobody”. Plus, if you doesn't appear as advertisement for a fan page, you don't encourage other people to add more private elements about their privacy.

Also, change the automatic tagging notification for photography if it's off. If a friend post a picture of you during a party for example, it can be negative for your reputation. You can't accept a tag before a photography is posted, so be vigilant.

Privacy, is not what people think in general. Phone number, home address, e-mail address, etc... are not a part of personality. These elements are between public and private area. But what you like, for example, food, games, country, etc are really a part of your personality. Firm like Facebook or Google can make statistic and profile to know who you are, as personality, not as who you are like your identity card says.

Be sure that personal data provided over Internet cannot be use to respond to your personal response which is used in case of lost password (Webmail for example). Social engineering is a manner to grab data by using public information or by lying to people in order to obtain information (phone to the target and be presented as a system administrator, etc...). It's used to penetrate a system or a particular target to be use later to penetrate other system. Hacker Croll, a french hacker, have use this to hack the Twitter account of the United State of America's president Barack Obama ! He have hacked the account of a Twitter administrator troughs a social engineering method on his webmail. The secret question has became public !

For Jean Marc-Manach (2010), the problem is between keyboard and chair ! You give by yourself your private data, so take care.

6.2 - In practice, what can I do ?

Your numeric identity

If someone want information on you, he will probably put your name and surname in Google. That is called “name Googling”. You can use multi-username to split information. You can have an anonymous blog on a multi-account hoster (to avoid the Whois research) to hide but express yourself. But, if you want a positive result in Google (and other research motors, but it's the most popular), you need to create your own numeric identity.

So, to control your numeric identity, one of the first thing to do is reserving your domain name, for example, firstnamename.com or firstname-name.com (and localization like .co.uk, .fr, etc). Nobody can use your identity and your mission in this case is to add positive elements about yourself. For example, your Curiculum Vitae (CV). If your pages are regularly updated, you will probably appears first on the Google results page.

Make links on this website in forum and professional blog you go on. Your peers will know you with the time and if your website is a blog, you can have a positive notoriety. That will also increase your Google rank and perhaps pass before a negative page about you. But don't spam too much, it can be negative for your reputation. If an article on your blog is not just (true), it's necessary to accept negative comments and, perhaps, do another article which explain what was your point of view when you have write this article, and if your judgment have change. Don't erase negative comment ! A blog can have a significant impact for your real and professional life, it's not only virtual. For this reason, some French famous blogger put their real name and are not anonymous.

If you see a negative article about you (Grégory Poui, 2007), try to contact the webmaster to erase it. You should be respected and that can engage an interesting conversation, and change mind. But you need to do that easy ! In other way, you can ask Google to don't indexing certain pages. There is a special defamation form for doing that. You can verify your reputation in real time by adding keywords in Google Alerts. That send you e-mail with corresponding links.

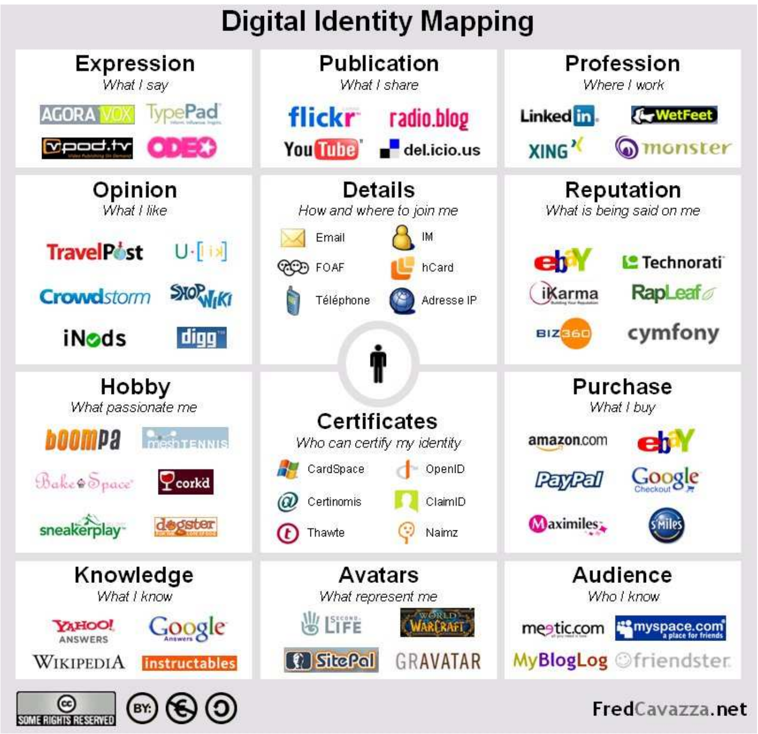


Illustration 4: Overall view of possible public life on the Web.

Software good practices

You need to learn how the operating system of your computer is working, and all electronic devices like game console and be aware and ready to install updates. A security issue is a potential risks for your personal data. Your software must be up-to-date, especially web-browser, instant messaging tools and every software which the Internet connection is normal to run, like a Tweeter client, Skype or Deluge.

To improve the security, software musn't be hacked and use illegally. Commonly, a key generator is a virus, replace dll files too. You must be vigilant when you download archives from unknown websites. If you download some popular software, be sure to download it from the official website or a popular download website (Not a direct download website like Rapidshare or MegaUpload but 01.net, Clubic, Download.cnet.com...). Because some software like Ccleaner have a not official and paid version as first results in Google. Web browser have now extension to prevent user from a risk and a safer navigation like Web-Of-Trust (WOT). It's an handmade extension to avoid errors in filtering.

If activities on a computer are just navigate on Internet, chatting on MSN, doing some basics stuff with Open Office, etc,.. A Linux based operating system is a great alternative to Windows (it cost nothing and can be tried without be installed on the computer with a live CD or Live USB Key). The number of threat is lower than on Windows but other things about privacy must be kept in mind.

6.3 - Password

That's an evidence, if your password is stolen, everybody can access to a lot's of private information with dangerous consequences on your life. Think about flight order, e-commerce order, taxes like DVLA for the government, etc... Your e-mail account is one of the most important things !

If your are developer, access to a system (or a website, etc...) must respect some principles. Technically, you have to store the login and the hash of login+password. A hash is the digital unique “fingerprint” of a data (here, text). On Internet, it's typically the MD5 algorithm. The algorithm is not reversible, so it's hard to find the password from the hash. The hash is composed of two things because rainbow table of password exist. A rainbow table is a dictionary of password with corresponding hash. The login is stored in clear in order to have unique user and avoid the technical problem of same login+password. The verification is made by calculating the hash of login+password given by the user and compare in the database to the corresponding user if exist. If it's equal, the password is correct.

The real password is hide trough the hash. It's important because in case of security failure, a black hacker can't use it directly. Plus, it's a protection for the user from the system administrator and the hierarchy. The password can be the same as a personal e-mail or Facebook account so it's better for the privacy to hide the password even from director and colleagues.

To finish, don't write your password on a paper. It's not safe. Avoid this behavior and try to remember your password for the same reasons as previously. If you have to think about a new password, try to use specific characters like @, $, £, &,... and numbers to enforce it. Plus, use the maximum characters possible. Don't use the same password for different websites/services, it's a big security hole. You can change just a part of a passphrase for example.

7 - Conclusion

We have seen that privacy comes from wide areas: just reflexion about our numeric identity, software update and control, networking website administration, private and public sphere differences,...

Mainly, a secure online life is mastered by the user himself. There is no easy and clearly way to learn how to protect our privacy, just experience and knowledge about tools used. Teenagers must be protected because they have to learn how it works and are an easy target.

Technically, security tools and operating systems have to be updated to prevent any problems. All passwords and personal data provided must be given or create with a maximum of attention.

In the future, threats about privacy have been a lot's discuss on Internet or illustrated trough films. Be aware about information technologies is needed to face new risks. Information website about technologies like http://privacy.org/, www.engadget.com, www.pcinpact.com (FR) or www.zataz.com (FR, specialized website about threats on Internet) can help you to understand new way in this area.

Also, if you have an access to the ACM, one of the most relevant book is “Privacy Actors, Performances and the Future of Privacy Protection” by Charles Raab and Bert-Jaap Koops or “Theory and policy in online privacy” by Sameer Hinduja. It's not focus on tool but more on theoretical aspect of privacy. They talk about privacy actors and how they works, what is the hierarchical field. Keep in mind that tool must be learn too to set your right exactly as you want, and, the most important, define by your own what is really your policy.

If, really, there are too much bad things about you on Internet, it exist specialized firms which can delete links by mediation, ask to justice or cover bad things into a mass of positive, neutral things and put them on the first place on Google. That type of firms begin to be know because of their communication like on the television news (TF1, 19/04/2010 20h).

Awareness + Security tools + Updates + Self questions + Strategy = Privacy controlled.

8 - References

[1] [Web page] [Fr] [2009] Serge Braudo

Définition de vie privée

Translation: Privacy definition (Available for french right)

http://www.dictionnaire-juridique.com/definition/vie-privee.php

Accessed on 04/02/2010

[2] [PDF] [En] [01/2010] Cross-tab for Microsoft

Online reputation in a connected world

http://go.microsoft.com/?linkid=9709510

Accessed on 04/02/2010

[3] [Book] [Fr] [2002] Laurent Chemla

Chapitre 8: "Liberté, égalité, responsabilité"

Translation: Chapter 8: "Liberty, equality, responsibility" (About: Internet economy, usage and evolution)

Confessions d'un voleur – Internet: La liberté confisquée

[Éditions Denoël] [ISBN : 2-207-25216-7] [B 25216-6]

Available online: *http://www.confessions-voleur.net/*

Accessed on 16/03/2010

[4] [Book] [Fr] [05/05/2009] Rémy Bigot, Jean-François Ruiz, Fadhila Brahimi, Antoine Dupin, Jean-Marc Manach, Christophe Blasquez, Emilie Ogez, François Mathieu, Lilian Mahoukou

L'identité numérique en question

Translation: About the numeric identity

Available online: http://www.scribd.com/doc/14983641/Lidentite-numerique-en-question

Accessed on 17/03/2010

[5] [TV documentary] [Fr] [18/03/2010] France 5

C'est dans l'air jeudi 18 mars 2010 (About consequences of a public life on Internet)

Translation: It's in the air

http://www.france5.fr/c-dans-l-air/index-fr.php?page=resume&id_rubrique=1394

Accessed on 19/03/2010

[6] [Book] [Fr] [19/03/2009] Nicolas Vanbremeersch

De la démocratie numérique

Translation: Some numeric democracy (About: Information transit, social web, public space)
[Edition Le Seuil] [ISBN-10: 2020987996] [ISBN-13: 978-2020987998]

[7] [TV documentary] [Fr] [29/05/2009] France 5

C'est dans l'air jeudi 29 mai 2010 (About possibilities for cops to go on your computer without your authorization)

Translation: It's in the air

http://www.france5.fr/c-dans-l-air/index-fr.php?page=resume&id_rubrique=1168

Accessed on 19/03/2010

[8] [Web Page] [Fr] [31/03/2010] Jean Marc-Manach

Vie privée : le problème se situe entre la chaise et le clavier

Translation: Privacy: The problem is between chair and keyboard

http://www.internetactu.net/2010/03/31/vie-privee-le-probleme-se-situe-entre-la-chaise-et-le-clavier/

Accessed on 19/03/2010

[9] [Web Page] [Fr] [15/03/2010] Marshall Kirkpatrick, Fabrice Epelboin

Facebook pourrait ouvrir ses données à l'occasion de la conférence F8

Translation: Facebook could open its data on the occasion of the F8 conference

http://fr.readwriteweb.com/2010/03/15/a-la-une/facebook-pourrait-ouvrir-ses-donnes-loccasion-de-confrence-f8

Accessed on 28/03/2010

[10] [Web Page] [Fr] [13/03/2009] Vincent Abry

25 trucs que Google connaît sur vous

Translation: 25 things Google knows about you

http://www.vincentabry.com/25-trucs-que-google-connait-sur-vous-4238/comment-page-1#comment-9921

Accessed on 28/03/2010

[11] [Web Page] [Fr] [29/03/2010] Vincent Hermann

Facebook : sites partenaires, géolocalisation et précisions

Translation: Facebook: partners, geolocalisation and details

http://www.pcinpact.com/actu/news/56111-facebook-politique-securite-critiques-avis-sites-partenaires-geolocalisation.htm

Accessed on 29/03/2010

[12] [Web Page] [Fr] [03/04/2010] Nil Sanyas

Édito : les questions secrètes, la fin des leaders et les Meuporg | Une question secrète qui n'a plus rien de secret

Translation: A secret question which have nothing secret now

http://www.pcinpact.com/actu/news/56228-edito-questions-secretes-leaders-meuhporgues.htm

Accessed on 03/04/2010

[13] [Web Page] [Fr] [26/03/2010] Jeff

Scotland Yard veut plus de contrôle dans les cybercafés

Translation: Scotland Yard wants more control in cybercofee

http://www.pcinpact.com/actu/news/56093-angleterre-police-cybercafes-controle.htm

Accessed on 26/03/2010

[14] [Web Page] [Fr] [25/03/2010] Nil Sanyas

Le pirate français de Twitter retrouvé et placé en garde à vue

Translation: The Twitter french hacker found and arrested

http://www.pcinpact.com/actu/news/56057-pirate-twitter-hacker-croll-comptes-obama-britney-spears.htm

Accessed on 25/03/2010

[15] [Web Page] [Fr] [25/03/2010] Nil Sanyas

Hacker Croll : "J'ai voulu passer un message aux Internautes"

Translation: Hacker Croll: "I wanted to spend a message to the Internet users"

http://www.pcinpact.com/actu/news/56071-hacker-croll-twitter-voila-voila-voila.htm

Accessed on 25/03/2010

[16] [Web Page] [Fr] [28/03/2010] Julien Dassonval

Facebook va de nouveau jouer avec vos données privées

Translation: Facebook will play with your private data again

http://blog.juliendassonval.com/marketing/facebook-va-de-nouveau-jouer-avec-vos-donnees-privees

Accessed on 28/03/2010

[17] [Web Page] [Fr] [21/11/2007] Grégory Poui

Votre identité numérique sur Facebook peut vous nuire…

Translation: Your digital identity on Facebook can damage you...

http://gregorypouy.blogs.com/marketing/2007/11/votre-identit-n.html

Accessed on 31/03/2010

[18] [Web Page] [Fr] [18/03/2010] Jean-Marc Manach

Vers une vie privée en réseau

Translation: Towards a private life in network

http://www.internetactu.net/2010/03/18/vers-une-vie-privee-en-reseau/

Accessed on 28/03/2010

[19] [Web page] [Fr] [26/03/2010] Sébastien Sauvage

Les certificats numérique ne suffisent plus

Translation: Numeric certificate are not more enough (Talk about numeric identity and certificate fail)

http://sebsauvage.net/rhaa/index.php?2010/03/26/12/03/17-les-certificats-ssl-ne-suffisent-plus

Accessed on 28/03/2010

[20] [Web page] [En] [24/03/2010] Seth Schoen

New Research Suggests That Governments May Fake SSL Certificates

http://www.eff.org/deeplinks/2010/03/researchers-reveal-likelihood-governments-fake-ssl

Accessed on28/03/2010

[21] [Web page] [Fr-En] [2010] Fabrice Prigent

Blacklists (About what website can be filtered in a public network)

http://cri.univ-tlse1.fr/blacklists/

Accessed on 28/03/2010

[22] [Web page] [Fr] [02/04/2010] Dimitri T.

Stage de citoyenneté pour diffamation sur Facebook

Translation: Training course of citizenship for defamation on Facebook

http://www.generation-nt.com/facebook-reseau-social-diffamation-propos-homophobes-stage-citoyennete-eleves-colleges-actualite-990701.html

Accessed on 02/04/2010

[23] [Web page] [Fr] [02/04/2010] Jérôme G.

La suppression d'Adobe Reader recommandée

Translation: The uninstall of Adobe Reader recommended

http://www.generation-nt.com/adobe-reader-fsecure-securite-actualite-990851.html

Accessed on 02/04/2010

[24] [Web page] [En] [05/04/2010] HiTechno Corner administrator

10 safety tips on Twitter

http://hitechnocorner.blogspot.com/2010/04/10-safety-tips-on-twitter.html

Accessed on 06/04/2010

[25] [Web page] [En] [15/01/2009] Peter Shankman

Be careful what you post ! (Another story with Twitter, the response is really interesting.)

http://shankman.com/be-careful-what-you-post/

Accessed on 29/03/2010

[26] [Web page] [Fr] [22/10/2006] Frederic Cavazza

Qu'est-ce que l'identité numérique ?

Translation: What is the numeric identity ?

http://www.fredcavazza.net/2006/10/22/qu-est-ce-que-l-identite-numerique/

Accessed on 29/03/2010

[27] [Web page] [Fr] [21/01/2009] Eric Dupin

Identité numérique : 10 règles simples pour contrôler son image sur internet

Translation: 10 simple rules to control your numeric identity on Internet

http://www.presse-citron.net/identite-numerique-10-regles-simples-pour-controler-son-image-sur-internet

Accessed on 29/03/2010

[28] [Web page] [Fr] [19/03/2010] Eric Dupin

Vous voulez perdre votre job? Utilisez Twitter

Translation: You want to lose your job? use Twitter

http://www.presse-citron.net/vous-voulez-perdre-votre-job-utilisez-twitter

Accessed on 02/04/2010

[29] [Web page] [Fr] [19/01/2009] RTL Info

Dérives de Facebook: On lui montre ses fesses lors d'un entretiens d'embauche !

Translation: Facebook deviation: We show him his buttocks during a job interviews!

http://www.rtlinfo.be/info/archive/211684/derives-de-facebook-on-lui-montre-ses-fesses-lors-d-un-entretien-d-embauche-!

Accessed on 26/03/2010

[30] [Web page] [Fr] [25/03/2010] Damien Bancal

Hacker Croll arrêté

Translation: Hacker Croll arrested

http://www.zataz.com/news/20044/hacker-croll--hackercroll--hacker-croll.html

Accessed on 26/03/2010

[31] [Web Page] [En] [18/01/2010] Casey Lynn

Lawyer's Bosses Don't Like Her Porn

http://www.geeksaresexy.net/2009/01/18/lawyers-bosses-dont-like-her-porn/

Accessed on 18/01/2010

[32] [Web Page] [En] [31/03/2010] Lee Mathews

Using FoxIt because you think it's safer than Adobe Reader? Think again.

http://www.downloadsquad.com/2010/03/31/using-foxit-because-you-think-its-safer-than-adobe-reader-thin/

Accessed on 31/03/2010

[32] [Book] [En] [15/10/2004] Sameer Hinduja

Theory and policy in online privacy

[The ACM] [ISSN: 0897-1986 (Print) 1874-6314 (Online)]

[34] [Book] [En] [14/11/2007] Xiaoyi Yu and Noboru Babaguchi

Privacy Preserving: Hiding a Face in a Face (About video recognition area)

[The ACM] [ISSN: 0302-9743 (Print) 1611-3349 (Online)]

[35] [Book] [En] [29/05/2009] Charles Raab and Bert-Jaap Koops

Privacy Actors, Performances and the Future of Privacy Protection

[The ACM] [ISBN: 978-1-4020-9497-2 (Print) 978-1-4020-9498-9 (Online)]