Digital Privacy and Cryptography

Dallas J. Fraser[1]

December 3, 2014

[1], Department of Physics and Computer Science, Wilfrid Laurier University, November 22, 2014

Abstract

Do people care about digital privacy and how can cryptography keep digital information private

Keywords: Digital Privacy, Cryptography, Privacy enhancing technologies (PET),

1 History of Growth and loss of Privacy

Digital privacy refers to collection and security of digital information that is quite personal in nature. A brief history of digital information helps show how digitial privacy has been changing recently. The growth of the Internet in the 1990's raised communication to a global level. It has changed society in many different aspects such as culture, communication, games, and even business. New industries were created by the internet, lead by new companies such as Google, Apple, and eventualy Facebook.

The development of databases, the growth of mobile industry and the increase usage of the Internet have resulted in a huge collection of personal data. More companies are moving their Information Techonology to the cloud and are creating Data

Centers which store an inconceivable amounts of data. "The company (facebook) claimed to have over a 100 petabytes of photos and video." [**?**]. This along with a strong developer community has lead to anyone being able to create a web application. There are tons of web based hosting companies such as Heroku which allows any to publish their web application easily.

2 Do People Care?

People are constantly giving out personal information such as email, address, and credit card daily through various websites. All kinds of information is being tracked when browsing through Google analytics. With all this information being shared and stored everyday, are people concerned with its security?

A recent study performed by Pew Research Center had a study on "Public Perceptions of Privacy and Security in the Post-Snowden Era". The two most intersting results were "80 percent of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites" and "70 percent of social networking site users say that they are at least somewhat concerned about the government accessing some of the information they share on social networking sites without their knowledge." [6]. This shows that the majority of people are concerned about privacy. These concern is most likely founded upon the recent news reports such as Snowden reports and the large collection of celebrity hacks. A lack of understanding of how techonogies work and the security behind lends a hands as well.

The Pew study was based in America but Canadians have similar feelings. Taking a look at Canadian politics where the privacy laws are being challenged. "As orga-

nizations find new ways to profit from personal information, the risks to privacy are growing exponentially," says Commissioner Stoddart [14]. Europre is more concerned thatn North America and recently challenged search companies especially search giant Google. "The European Parliament has passed a historic vote to break up US tech giant Google."[15]. This is on top of the fact that Google and EU are in the middle of a four year long dispute about anti-trust laws.

It is evident that people are concerned about digital privacy. However, this seems to contradict the behaviour of people, where countless of private photos are uploaded and personal messages sent everyday. "Most say they want to do more to protect their privacy, but many believe it is not possible to be anonymous online"[6]. Most consumers feel that protecting their information is too difficult and their rights as a consumer are non-existence.

3 Digital Privacy Supply

The developer community and business are one creating the applications which collect the data. Increase in techonologies allows for developers to create and publish webites in a short time. This is evident in hackathons where website are created in a weekend. Engineering processes are evolving to help encourage rapid change and this is seen through Agile development. Is security is a major concern for businesses in this process and do they meet consumer demands?

There is a lack of legislation. This is largely due to the how fast these techonologies have grown and how slow the political systems moves. Most of contract law is obsolete when it comes to the Internet and Internet transactions. Canadas Anti-Spam Legislation (CASL) which was passed in Decemeber 2010 but not enforced until July

1, 2014 [13]. It took about a decade and a half to create a spam law and another four years to implement it. This lack of legislation allows for companies to freely deal with their data, and user' agreements with little government interference. The goverment is doing little to ensure digital privacy and in certain cases in exploiting personal information in the name of security. A recent example is the N.S.A complaint about Apple's Iphone encryption of data where the user's password was used to encrypt the data [10]. Encryption is more a hassle and back doors make their job much easier.

All business have the incentive to improve profit and without external incentives will strictly focus on profits. The two greatest external forces on corporations is government and public opinion. The government pressure on companies is non-existence and what force that is present is outdated. The public is less concerned about with drawbacks of the data privacy and more concerned with the benefits of the application. Most people ask what can it do for me instead of how does it work and what security measures are in place? These lack of incentive have lead to business tending to focus more what profit can be produced from personal data and not the long term impact it could have. There is a lack of research done by the companies producing these techonologies on the users. The negative side effects are not taken into consideration during the design process. Security is usually an after thought and privacy is never considered. This is evident in a recent study done by Cisco Canada in which they found "40 per cent of about 500 firms surveyed had security strategies" [16]. Just last week, Sony was hacked where a significant amount of employee information was leaked. Their are estimates of "100 terabytes of data" leaked containing information such as "list of employee salaries and bonuses; Social Security numbers and birth dates; HR employee performance reviews, criminal background checks and termination records" [19].

The demand of digital privacy is greater than the current supply of security. The lack of legislative and consumer pressures have prevented companies from increasing their level of security. This has resulted in insecure websites and vulnerable private information.

4 Need for Change

The lack of security is a concern for most people. People's personal information may be vulnerable but does this matter?

The culture changed started by the Internet has brought new social issues. Now a citizen is evaluated by their on-line social interaction. Companies will use Facebook, LinkedIn and Google to screen out potential candidates. Employers need to monitor the social lives closely because of this. One cyber attack can greatly damage one reputation and may threaten their employment or even their employability. The other thing is the Internet does not forget about past mistakes. A good example of this is the recent firing of a Quebec teacher. "The availability on the Internet of erotic films in which she acted created an entirely new context that was not ideal for our students" [17] was the reason for her dismissal. This problem will only get larger as more information is stored and moved into an age where all data becomes digitalized.

The new buzz in the business world is big data and processing big data for applications. The applications are used by business to make decision and to help better market their product. There is a big push for all companies to collect data and analyzing this data to get ahead. Their are large claims by people of all the potential including big data making people happy [18]. The collection of this data has little regulations and with an increasing financial incentive it can or may cause some business

to collect this information in unethical ways. The other problem is the over confidence in this new field. Micheal Jordan a Professor at the University of California stated that "When you have large amounts of data, your appetite for hypotheses tends to get even larger. And if its growing faster than the statistical strength of the data, then many of your inferences are likely to be false. They are likely to be white noise." [3]. Google Flu Trends is a system Google has developed for tracking the flu. "Google Flu Trends is often held up as an exemplary use of big data" [5]. It was reported that "GFT was predicting more than double the proportion of doctor visits for influenza-like illness (ILI) than the Centers for Disease Control and Prevention (CDC)," [5]. This is a good case example of how big data does not have all the answers and is a field needs improvement and reasearch. Over confidence in it could lead to costly mislead decisions based on "big data hubris" [5].

The rise of social reputation and impact on lives raised the need for security. The lure of big data entices companies to quickly convert implement big data storage and collection. The lure of big data possibilites sometimes overshadows security and digital privacy. Security and digital privacy should be more important that big data and its applications. "If I have no principles, and I build thousands of bridges without any actual science, lots of them will fall down, and great disasters will occur" (Micheal Jordan)[3].

5 Ways to Change

It is clear that security and digital privacy need to be focused and strengthened. A developer needs to recognize this during the design of their system. They need to build into their system ways users can stay annonymous or delete private information when requested. Digital privacy should be the standard when creating web applications and

a feature. What techonlogy can help developer keep personal information private?

There a wide range of Private Enhancing techniques using Crypotgraphy. This paper will focus on Private Digital Credentials, Type X remailers, and Onion Routing focusing on how these can allow of digital privacy.

6 Private Digital Credentials

What is it?

How does it work?

How does it provide digital privacy?

7 Type X Remailers

What is it?

How does it work?

How does it provide digital privacy and its benefits?

8 Onion Routing

What is it?

How does it work?

How does it provide digital privacy and its benefits?

9 Conclusion

Do it obvisouly

Acknowledgement

This work was done by author D.J.F. in partial fulfillment of the course requirements for CP460: Applied Cryptography in the Department of Physics and Computer Science at Wilfrid Laurier University.

References

[1] Albergotti, R. (2014, November 13). Facebook Gives Its Privacy Policy a Makeover. Retrieved November 16, 2014, *http://blogs.wsj.com/digits/2014/11/13/facebook-gives-its-privacy-policy-a-makeover/*

[2] Doctorow, C. (2014, November 12). Peak indifference-to-surveillance. Retrieved November 14, 2014, *http://boingboing.net/2014/11/12/peak-indifference-to-surveilla-2.html*

[3] Gomes, L. (2014, October 20). Machine-Learning Maestro Michael Jordan on the Delusions of Big Data and Other Huge Engineering Efforts. Retrieved October 26, 2014, *http://spectrum.ieee.org/robotics/artificial-intelligence/machinelearning-maestro-michael-jordan-on-the-delusions-of-big-data-and-other-huge-engineering-efforts*

[4] Lawton, V. (2013, May 23). New privacy challenges demand stronger protections for Canadians. Retrieved October 14, 2014

[5] Lazer, D., Kennedy, R., King, G., and Vespignan, A. (2014, March 14). The Parable of Google Flu: Traps in Big Data Analysis. Retrieved November 17, 2014.

[6] Madden, M. (2014, November 12). Public Perceptions of Privacy and Security in the Post-Snowden Era. Retrieved November 15, 2014, *http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/*

[7] Notley, T. (2014, August 4). Why digital privacy and security are important for development. Retrieved October 14, 2014, *http://www.theguardian.com/global-development/poverty-matters/2011/aug/04/digital-technology-development-tool*

[8] Nowak, P. (2014, June 21). In era of revelation, privacy more important than ever. Retrieved October 14, 2014, *http://business.financialpost.com/2012/06/21/in-era-of-revelation-privacy-more-important-than-ever*

[9] Roughol, I. (2014, November 19). Uber's Privacy Scandal Is a Failure of Culture. Retrieved November 19, 2014, *https://www.linkedin.com/today/post/article/ubers-privacy-scandal-failure-isabelle*

[10] Schneier, B. (2014, October 6). IPhone Encryption and the Return of the Crypto Wars. Retrieved November 23, 2014, *https://www.schneier.com/blog/archives/2014/10/iphone _encrypti _1.html*

[11] Solove, D. (2014, November 12). People Care About Privacy Despite Their Behavior. Retrieved November 13, 2014, *https://www.linkedin.com/today/post/article/20141112171953-2259773-people-care-about-privacy-despite-their-behavior*

[12] Wallbank,P. How much server space do Internet companies need to run their sites? *http://paulwallbank.com/2012/08/23/how-much-server-space-do-internet-companies-need-to-run-their-sites/* (2012)

[13] Fast Facts. (2013, December 4). Retrieved November 23, 2014, *from http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html*

[14] Lawton, V. (2013, May 23). New privacy challenges demand stronger protections for Canadians. Retrieved October 14, 2014, from https://www.priv.gc.ca/media/nr-c/2013/nr-c _130523_e.asp

[15] Cook, J. (2014, November 27). The European Parliament Just Voted To Break Up Google Read more: Http://www.businessinsider.com/european-parliament-voted-to-break-up-google-2014-11ixzz3KhLx0CEU. Retrieved November 28, 2014, from http://www.businessinsider.com/european-parliament-voted-to-break-up-google-2014-11

[16] Blackwell, R. (2014, December 2). Many Canadian firms are unprepared to face cybersecurity attacks: Study. Retrieved December 2, 2014, from http://www.theglobeandmail.com/report-on-business/smaller-canadian-firms-less-prepared-for-threat-of-cyberattack/article21857498/

[17] Peritz, I. (2014, October 20). Montreal teacher, 73, loses job over film nudity more than 40 years ago. Retrieved December 2, 2014, from http://www.theglobeandmail.com/news/national/montreal-teacher-73-loses-job-over-film-nudity-more-than-40-years-ago/article21183669/

[18] Banayan, A. (2014, November 4). 2 Ways Big Data Can Make You Happier. Retrieved November 5, 2014, from https://www.linkedin.com/pulse/article/20141104090919-80844253-2-ways-big-data-can-make-you-happier?trk=tod-home-art-list-large_0

[19] Zetter, K. (2014, December 3). Sony Got Hacked Hard: What We Know and Dont Know So Far. Retrieved December 3, 2014, from http://www.wired.com/2014/12/sony-hack-what-we-know/

[20] Goldberg, I., Wagner, D., and Brewer, E. (1997, January 21). Privacy-enhancing technologies for the Internet. Retrieved December 3, 2014, from http://www.cypherpunks.ca/ iang/pubs/privacy-compcon97.pdf

[21] Goldberg, I. (2007, December 1). Privacy Enhancing Technologies for the Internet III: Ten Years Later. Retrieved December 3, 2014, from http://www.cypherpunks.ca/ iang/pubs/pet3.pdf