Online Privacy: Why You Should Care

Don Jacob

Billy Graham once said, "Once you've lost your privacy, you realize you've lost an extremely valuable thing" (www.brainyquote.com/quotes/quotes/b/**billy**graha446542.html). Privacy is highly valued in USA and similar nations. The concept of privacy could differ from nations to nations and from community to community. Thus, privacy is defined in several ways

and there may not be any unanimity of views. In this paper a discussion on a narrower topic of *Online Privacy* is presented.

Slow Loss of Privacy in Online

With all the technological advances and the ever-increasing usage rates of online services and programs, privacy is slowly given away. Every time you begin using an online service such as *Google's email* or the online social network such as *Facebook,* you open a gateway for information to be leaked out by you and of you into the public domain.

Importance to Safeguard Online Privacy

The idea of maintaining online privacy is something that is not given much thought by majority of users. The reason is that most users don't realize that this information, for example, a location attached to a status or checking into locations can be used by stalkers and other undesirable people to track your whereabouts. You might accidentally alert a stalker where you are going or accidentally inform a burglar that your home is vacant long enough for them to steal whatever they are after.

There are a lot of people that use online services from websites like **Google** and social networks like **Facebook**. However, many fail to realize their privacy in the domain of online is dwindling. We need to take action to keep ourselves protected from prying eyes.

Online Privacy

Our privacy is being attacked everyday on multiple fronts but I will be discussing in specificity our privacy online.

Many users don't realize the amount of information they are truly giving away (MSNBC, Sullivan). They especially don't realize how many people have access to their information. A popular service to use today is *foursquare*, an app where you go and specifically check in to a physical location and in addition to that you can have it setup to automatically to post on Facebook and thereby share your location to everyone you know or make that info public. You may receive coupons and offers for checking in. But is allowing others to track you really worth the minimal offers on things that you can go without or afford to pay in full?

Concept of Privacy

Before I go any further I should explain the definition, the concept of privacy. The definition and concept of privacy is debated. Privacy is considered to include these aspects: interferences with personal information, secrecy, repose, reserve, peace, of mind, bodily integrity, anonymity, solitude, seclusion, sanctuary, intimacy or intimate relationships, and decisional autonomy. Put simply, the definition or the concept of privacy is a conditional or limited access to one or more aspects of a person (Powers, 370-371).

Customized Needs for Privacy

Now everyone enjoys privacy and everyone desires it. The needs of privacy are customized to each individual as their personal preference for giving an individual or group limited or full access to the info on the aspect of the distributer's life (Privacy and the Right to Privacy, McCloskey).

An illustration of how privacy works is that a person may have a house, there is one central room with access to various sub rooms around it. In each sub room is a part of the person. For example one sub room may contain the part of a person's physical image, the other room may contain the part of a person's personal or private behaviors or tendencies, and the other room may contain the part of a person, that is, their interests. Now each sub room has a door to the outside world, the person who lives in this house chooses who can enter and who can observe the things in each sub room. That is where the conditional or limited access definition can be

seen. Now in the center of the house where the main room is, is where the conscious being of the person resides. The conscious being never leaves that room because there are certain things that others can never know or truly understand in the exact same way as the person who lives in that house (Bates 430).

Inadvertent Leak

Now that you have an understanding of what privacy is and how it works imagine that you inadvertently leave the door bridging the outside world and your sub room open, or that you accidentally forgot to lock the door. That means you have let some information escape, you have let unwanted or undesirable people, groups, organizations, etc. into your personal life and they now know and have access to information about you that you didn't want them to know. This is what is constantly happening in today's world.

No Private Information is Trivial

People are blinded by the possibilities and offers they can receive and benefit from by giving others information about them (Scu.edu, Raicu). Giving others that information at the time may seem trivial and incapable of harming them, but there is a reason they want that 'trivial' information. If that information didn't have any value to others why would they want it?

The thing is that people provide websites, social networks, connected media, etc. a reusable ticket to allow that company/organization to have access to and use their information when they begin using that service. After they accept the agreements those organizations/companies no longer require your consent every time you use the service, in fact they even have access when you are not using their service.

Granting Access

On the topic of granting access to services to view and use your personal information, there are also a large number of other services and apps that use your preexisting account to

make a sub account on their service. It initially seems like a great idea and it is when you consider that this eliminates the need for numerous accounts being made for all the applications and services you use. However, there is a down side to linking an app such as a game or another app you use to browse things that you may not want everyone to know about.

When you begin using another service by telling it to make a sub account off of your existing **Facebook** or **google**+ account, those services will have access to all the information about you such as your birthdate, your picture, your place of work or study, and your contact information. In addition to that the services can monitor your posts and in some cases make posts or changes on your **Facebook** account on your behalf. They also have access to your friends list and can contact your friends.

The Purpose

The main purpose for this is for the service to advertise using your account as a medium and also advertise to your friends and acquaintances. The majorities of services don't use your information against you or make you look bad but the unaware user can accidentally grant access to someone who can steal their information and cause a case of identity theft. Many organizations and services that are for social purposes also sell your usage statistics and some types of information under an anonymous name for the companies who buy it to analyze and find trends, etc.

Speaking of services and organizations, Google is one of the largest and fastest growing organizations in the world and they provide numerous services. Google is known to everyone capable of using a computer and the Internet. They have numerous services, products, and a very large group of email users (Wired, Levy). The thing that is so attractive about Google is their eco system. Originally they started out as just a search engine 14 years ago and now they have expanded to include most notably: advertising, email client, cloud working station (Drive), android operating system, mobile devices, wearable technology, computers, web browsers, YouTube, Motorola, Inc. etc. The list goes on and on. With one account you essentially have

access to every feature and service that is offered. Not to mention the ability to link services from other vendors via Google's social network **Google+**.

Google Operations

Google is great; they are the center for us to go for almost anything, but, with such a massive organization in so many different fields, there is an increasing fear of Google in some way taking over the society. A few years ago it was discovered that Google's servers were reading all the emails received and sent by Gmail users to search for key words and offer deals and advertising based on their email texts (Google's Dominance, Hatch). This wasn't illegal as it was stated in their user agreement, however many people were shocked and a few outraged. They technically shouldn't be surprised as it was the user's duty to read the agreement and understand it before using the service. Google still continues to do this however their tactics for advertising have rapidly changed. In addition to reading emails their servers also advertise by providing paid results near the top of popular queries in their search engine, show relevant ads on the sides of webpages based on your browsing history. Your usage of the Internet is tracked in almost every way and Google pays a huge roll analyzing and generating ads on their websites and others who pay Google to advertise for them on their sites and in searches.

These anonymous monitoring procedures of computers on users of Google and even more importantly the Internet itself are seen as a large threat towards our privacy and safety of our information.

Many Benefits

There are good things that have resulted from Google's massive presence and their numerous services. For example there is Google Drive, a service that can store a wide variety of work related files and even media files as well. It also provides you with the ability to access, edit, and create common documents. This has greatly helped the business and education industry, especially the ability to share and co-create and edit documents. The best part is it is all for free.

All of these free and useful functionalities present and available are wonderful for the public but at what cost?

Nothing *Is* Ever Free

Nothing is ever free in this world; someone is also paying for something. You are paying for Google's free ecosystem by using their services and viewing ads from other companies. Now you don't have unlimited storage, you are given a portion of storage for free and then given the option to pay monthly or yearly for additional space. I have 15GB of free space for storage of files for example, of which I am only using 3 GB of the 15GB at the moment. This amount of storage is for google drive only and there are other amounts of storage available per service as predetermined by Google. Whether a person choses to use Google's eco system or not is up to them. However, it is good to remember that there is always the possibility of losing your privacy.

Government and Privacy

At this point it is not an issue with the government not regulating properly. It is not that the organizations have banded together to take over society either. This is not to say that the organizations have done no wrong or that the government hasn't done its fair share of invasion of privacy either. The main leading cause, the reason we are here in this predicament is mainly no one else's fault but you and me (A Loss of Privacy: The Fault Lies With Us, Greenbaum). It was and is our duty, the users of the services and networks available.

Full Access to Our Lives in Gradual Progression – The End User Agreement

This was not a change or trend that began overnight but a gradual progression. One little change at a time the government and organizations moved closer and closer to having full access of our lives. The reason the majority never saw it coming was that the organizations slowly and skillfully integrated their policy changes in the end user agreements. The end user agreements are those long articles, usually 30-80 pages long and are essentially contracts. No one ever takes time to read them. Furthermore, the fact of the matter is that the language and terminology used

in these long articles are normally far above the reading level of your average user. In addition to that the transition is being made for people to not even have to open the agreements and simply offered small links so that they can skip it all together. Likewise there have been legislation and laws that have been put in effect as well to allow the government to use their resources and various branches to use their powers to conduct scans and observations of random individuals as well. The government has made their fair share of blunders and have misused their abilities; the NSA being the one to commit the largest scams (Ted.com, Hypponen).

A Notable Experiment

There was an experiment done YouTuber named Jack Vale, in his video he used his phone to log into his own Instagram account and looked up people who posted to **Instagram** recently around him. Instagram is a social media site where users take and edit photos and then share them to either their followers or make them public. In addition **Instagram** allows you to attach locations along with the photos and also post these photos with locations to other sites like **Facebook** and **Google+**. Vale looked up pictures taken and posted nearby and then found the location and the person. He then presumed to ask them questions and talk about things he could find out by viewing the posters' accounts and their other photos and the text associated with their pictures (Social Media Experiment, Vale). This experiment of his is 100% legal and is a very strong example of what carelessly sharing vital information can do to you.

To Conclude

Privacy is a large topic and it is needless to say this research paper did not come close to covering it all, not even just privacy related to the Internet. However, from the examples given it is clear how over-sharing personal information can be very dangerous to your safety and the only way to protect yourself is to make those hard decisions on what information should be given away and what should stay private is up to you, the user.

Acknowledgement:

My grateful thanks are due to my teacher Professor Jennifer Miller for her encouragement and guidance.

===

Works Cited

Bates, Alan P. "Privacy-a Useful Concept?" *Social Forces* 42.4 (1964): 429-34. *JSTOR*. Web. 15 Nov. 2013.

Greenbaum, Dov. "A Loss of Privacy: The Fault Lies With Us." *The New York Times*. N.p., 13 Oct. 2013. Web. 12 Nov. 2013.

Hatch, David. "Google's Dominance." *Is the Online-search Giant Too Powerful?* 21.40 (2011): n. pag. *CQ Researcher Online*. Web. 14 Nov. 2013.

How the NSA Betrayed the World's Trust -- Time to Act. Prod. Ted Talks. Perf. Mikko Hypponen. *Ted.com*. Ted Talks, Nov. 2013. Web. 15 Nov. 2013.

Levy, Steven. "Google Throws Open Doors to Its Top-Secret Data Center." *Wired.com*. Conde Nast Digital, 15 Oct. 2012. Web. 01 Dec. 2013.

McCloskey, H. J. "Privacy and the Right to Privacy." *Philosophy* 55.211 (1980): 17-38. *JSTOR*. Web. 15 Nov. 2013.

Powers, Madison. "A Cognitive Access Definition of Privacy." *Law and Philosophy* 15.4 (1996): 369-86. *JSTOR*. Web. 15 Nov. 2013.

Raicu, Irina. "Loss of Online Privacy: What's the Harm?" *Scu.edu*. Scu.edu, June 2012. Web. 15 Nov. 2013.

Sullivan, Bob. "Privacy under Attack, but Does Anybody Care?" *Msnbc.com*. Msnbc.com, 17 Oct. 2006. Web. 15 Nov. 2013.

Vale, Jack. "SOCIAL MEDIA EXPERIMENT." *You tube*. Ed. David Cetani. Youtube, LLC,, 18 Nov. 2013. Web. 01 Dec. 2013.

www.brainyquote.com/quotes/quotes/b/**billy**graha446542.html

---

Don Jacob

djw1994@gmail.com