Privacy in the World

Ann Miyahara

Professor K. Cahill

CST 373 - Ethics in Comm. and Tech.

Assignment 5

Feb. 13, 2014

The concept of privacy continues to change every year, a large factor in the way it changes is due to technology. As technology evolves privacy lines blur more and more. What society considers private becomes public. Nothing is as private has people think, opinions are affected by new technology, often without consciously realizing it. However, privacy is protected only so far in some cases people have no privacy at all. Every country is different about how much privacy they allow their citizens. For example, China, in January a new regulation for Internet users was implemented, making all users required to register their legal names when they attempt to upload videos to Chinese video sites. China's State Administration of Press, Publication, Radio, Film and Television (SARFT) released a statement stating the new requirement was to, "prevent vulgar content, base art forms, exaggerated violence and sexual content in Internet videos having negative effect on society" (Reuters). The new rule comes at a time when the Communist Party is trying to tighten their control of the Internet and media to suppress anti-government sentiment.

Different countries consider privacy differently but the only way to have true and complete privacy is to stay indoors, away from technology. When people leave the security of their homes, they are allowing themselves to be watched and monitored. Many American cities are installing surveillance cameras in public areas such as parks and busy urban areas. These surveillance systems are put in place to help law enforcement prevent crimes from taking place and in the cases that it does not prevent the crime it can be used as a tool to solve the crimes. These surveillance systems use some of the same types of

technology that the New York Police Department uses to catch terrorists (Henn). The United Kingdoms has a massive collection of surveillance programs for their country. The British Security Industry Authority (BSIA), reports an estimate 5.9 million closed-circuit television (CCTV) cameras situated in what they call, “sensitive locations” these locations include schools and hospitals. Based on those numbers there is one camera for every 14 persons in the country. One citizen’s whole day can be caught on camera. There are between 291,000 to 373,000 camera’s in public schools, and anywhere from 80,000 to 159,000 in health centers or hospitals (Barrett). This is a huge privacy violation for the citizens of the UK but because there is such a fear of the attack on their public transportation and the past attack have happen. The citizens of the UK allow it and are even expect some type of search if the police find it necessary. The cameras are there to supposedly reassure the population that there is something being done to protect them and that their loss in privacy is necessary and rewarded. Cameras on the street give the appearance of safety, but it is because of these cameras that people behave lawfully in public, but it does not help in the privacy of their own home, their own personal domain. These surveillance tools are used to enforce lawful behavior, they act as a warning to people to behavior because they are being watch.

Although there are some laws protecting individual privacy to some degree, every country has its own values regarding what should be protected. What some consider private others may or may not and privacy laws are not as secure when compared to other foreign countries. The states in the European

Union have some of the strictest privacy laws in modern times. The laws outline very large fines when individuals are found guilty of breaking these laws, Spain and Germany have fines in the hundreds of thousand U.S. dollar ranges. Asia is quickly increasing their privacy laws, and in 2012 Singapore passed a data privacy law that protects all personal data for ten years after a person's death. Then there are the countries that have been slower to strengthen their privacy laws, Argentina for example is a country that was not in a hurry to make their privacy laws stronger until it became necessary for trade contracts. As for the U.S. we have privacy laws protecting healthcare information and financial data but little else. If a person goes to an online store before they can make a purchase that person must agree to the company's privacy policy. If that company breaks their own law then the U.S. Federal Trade Commission will step in but other than that, people are on their own. Some states have their own state level laws such as California and Massachusetts these laws are separate from the federal laws and are only applicable for consumer data problems taken place in that state (Gustke).

People wanting to keep their privacy really have to work hard to do so it is not a guaranteed thing anymore. In order to have some form of privacy for their online data. It must be encrypted; encryption is basically a way of protecting data while it is transferred to someone or somewhere else. It uses an algorithm that makes it difficult for someone to read the data without the right "key". For example Alice wants to send an email with private information to Bob. So Alice has a "key" that encrypts the email and when Bob gets the email he can decrypt

it with his “key”. Keep in mind this is one way to promote privacy but it is not a guarantee that the information will be kept a secret after all, the server is connected to your email provider who has access to your email account. However encryption is not always used for only protecting personal information it also used to hide dangerous data as well. Data that has the potential to harm citizens, encryption has become a powerful tool for criminals and terrorist to hide their dealings. Amitai Etzioni has a Ph.D in Sociology from the University of California, Berkeley and is the author of 24 books on economics, privacy, and sociology. Etzioni gives five threats encryption posed to law enforcement, public safety, and national security. They are:

> “1. Encryption can make it impossible to obtain necessary evidence.
>
> 2. Encryption can frustrate communications intercepts that reveal valuable information about the intentions, plans and membership of criminal organizations and generate leads for criminal investigations
>
> 3. Encryption can frustrate anti-terrorism efforts.
>
> 4. Encryption can hinder the gathering of intelligence.
>
> 5. Encryption, oddly enough, may lead to greater violations of privacy than would otherwise have occurred.”

(The Limits of Privacy, 77).

Privacy was in many ways much easier to provide and protect when technology was not so advanced as it is now. Before the Internet, privacy could be guaranteed. Internet search history, medical files, personal messages, to name just a few can all be accessed through the web. Even a game downloaded on to a mobile device requests access to your personal information. Everything a person is told not to do in person is forgotten once they go online. People talk to strangers and give out personal information; it is harder for people to maintain their privacy opinions when it is through a computer. When using the Internet people have to understand they have little to no privacy, every bit of data they give is public and anyone can find it. Social media is large factor in the privacy issue many do not even think about it, but a stranger can go onto someone's Facebook page and they can be located in a matter of minutes by the location updater option the site has for users. A Google map pops up and a red flag points to that person's current location. It is not a vague location either, it tells you if it is a hotel, restaurant, store, or anything else. Most people do not think about that as being an invasion of privacy. Yet if a stranger were to walk up to someone in public and ask where that person was just at it would then be an invasion of privacy. It is yet another way of being tracked. The amount of websites selling people's personal data is unbelievable. Not that you really need to buy the information now when just browsing through a user's social media accounts and it is unfortunately very easy to get an idea of a person's personality and "…by observing Internet use, we can gain insight into how things such as the onslaught of information from television, print, and even the Internet itself can

change behavior" (Tancer, "Click", 59). Bill Tancer, an expert on online behavior, makes a point in his book how easy it is to track a trend. By taking peoples search results the company can see which month has the most search for prom, January is the month with most prom related searches. This helps companies make more of a profit by having merchandise ready at peak times when it is needed. It does not stop there, the person's data is taken and sold to other, third party companies; this turns the people from customers to merchandise. Tracking customers has become very easy, there are the cellphones, navigation devices, and cameras, all have the capability to trace an individual. The government uses these tools often to track down people of interest. Last year, a few short months ago the news reported that The National Security Agency (NSA) has been collecting hundreds of millions of electronic communications each day from American citizens. These included audio, video, photographs, emails and searches from Microsoft, Google, and many more. All of this is to help detect suspicious behavior (Jakes). The fact of the matter is that the privacy of United States citizens was violated and the President told the people they had to essentially put up with it so they would be protected from future terrorist attacks.

September 11, 2001 was a time of change for Americans and their privacy. With the fear of another attack many citizens are more willing to release the privacy rights in return for a safer county. Etzioni wrote that people are willing to, "…give up rights in order to fight terrorism, and their perception of whether or not they will need to give up some of their own rights, is also tied to their level of fear" ("How Patriotic is the Patriot Act?", 16). Studies show that citizens are very

fickle when it comes to allowing their rights being changed or put aside for a time. When asked, citizens were willing to give up more rights if told it would be a necessity, more than six out of ten were willing. Two months later the numbers did decrease some; more than 5 out of ten were willing. As the fear decreased so did the peoples need to agree with the government on the invasion of privacy issue. In an article published by the Washington Post in July of, 2013 it is stated that, “about four out of ten say it is more important to protect privacy even if that limits the government’s ability to investigate possible terrorist threats” (Cohen).

A good example of how privacy laws are changing would be the airport after the attack on 9/11, the airlines tightened security considerably and many did not approve of the new regulations. People could be checked for any reason, and with cameras and scanners security has become invasive. Body scanners have taken away a person’s privacy when it comes to their body. The images from the machine were very graphic and were dubbed by many as a “virtual strip search”. The machines were invasive and disturbed travelers but there was nothing they could do right away. In January of 2013 CNN reported that the machines were going to be replaced by another machine that “displays a generic outline of the human body” one that raises fewer privacy concerns (Ahlers).

When it comes to privacy around the world, different governments have different ideas on how to provide it to the citizens of their country while still protecting them from what they believe are threats to their safety. And people around the world have their own ideas about how the government should protect them while still giving them their liberties; however, with so many potential

attacks as a possibility, it is hard for the government to provide this. When being compared to other countries, the people of America can be consider as having more control of their privacy even with the reports of secret monitoring that is taking place. Considering other countries such as China where their people can be put in prison for publically speaking their minds. In Israel the citizens of this country have the Protection of Privacy Law and Human Dignity, and Liberty law. Although they are there to protect the people's rights they can be easily put aside when criminal justice needs come into the picture. It is easily seen how many liberties Americans truly have in comparison. But the government should be more understanding to the people when it comes to their privacy. They do not want their private conversations and messages to be seen by anyone with clearance to view the stored data.

It is impossible to define privacy; there are many interpretation of the concept. Each person's view is different, based on their own culture and their own understand of their rights. Many countries' constitutions do not mention at all and some indirectly. This allows the government to tell its people how they should interpret it. The way things are going the government is going to continue to put the country's security before that of its people's privacy. In a press conference, the President of the United States makes it clear that he will always side with the protection of the country rather than the people's privacy. He believes the people of the United States should support all branches of law enforcement in any way they can, "U.S. national security is dependent on those folks being able to operate with confidence that folks back home have their

backs, so they're not just left out there high and dry, and potentially put in even more danger than they may already be" (Cillizza). The people of this country allow fear to motivate them to take the same view on privacy as the government does. They feel for the most part they have nothing to hide so why make a big deal out of something as little as individual's privacy. But it is a large issue with the people do not fight for their own liberty then how much more will they lose.

Article 12 in The Universal Declaration of Human Rights states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks" (Universal Declaration of Human Rights). From reading this it says that every person has the right to be protected by law enforcement, that their privacy, family, home, correspondence, honor, and reputation is protected yet the people who are supposed to protect them are spying on them. It is a universal right that should be followed. Yet everyday citizens are allowing this right be broken by their own government. If people do not stand up for their rights then all of their liberty will be lost without a fight. This leaves the people to be controlled by their government instead of the government being controlled by the people.

Citations

Ahlers, Mike M. "TSA Removing 'virtual Strip Search' Body Scanners." *CNN*. Cable News Network, 19 Jan. 2013. Web. 28 Feb. 2014.

Barrett, David. "One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey." *The Telegraph*. Telegraph Media Group, 10 July 2013. Web. 01 Mar. 2014.

Cohen, Jon, and Dan Balz. "Poll: Privacy Concerns Rise after NSA Leaks." *Washington Post*. The Washington Post, 25 July 2013. Web. 28 Feb. 2014.

Cillizza, Chris. "In the Battle between Privacy and Security, Security Always Wins."*Washingtonpost.com*. The Washington Post, 6 June 2013. Web. 28 Feb. 2014.

Etzioni, Amitai. “Biography.” *Amitai Etzioni.* Version 1. Web. 3 March 2014.

Etzioni, Amitai. *How Patriotic Is the Patriot Act?: Freedom versus Security in the Age of Terrorism*. New York: Routledge, 2004. Print.

Etzioni, Amitai. *The Limits of Privacy*. New York: Basic, 1999. Print.

Gustke, Constance. "BBC Capital." *BBC Capital*. BBC.com, 26 June 2013. Web. 26 Feb. 2014.

Henn, Steve. "In More Cities, A Camera On Every Corner, Park And Sidewalk." *NPR*. NPR, 20 June 2013. Web. 24 Feb. 2014.

Jakes, Lara, and Darlene Supervilla. "Obama Defends NSA, Says America Has To Make Choices Between Privacy And Security." *The Huffington Post*. TheHuffingtonPost.com, 07 June 2013. Web. 01 Mar. 2014.

Reuters. "Chinese Must Now Post Online Videos Under Their Real Names." *The Huffington Post*. TheHuffingtonPost.com, 21 Jan. 2014. Web. 23 Feb. 2014.

Tancer, Bill. *Click: What Millions of People Are Doing Online and Why It Matters*. New York: Hyperion, 2008. Print.

“Universal Declaration of Human Rights.” *UN Briefing Papers/Human Rights.*1948. United Nations. Web. 29 Feb. 2014