Luke Pederson

CST 373 - Ethics

Professor Kevin Cahill

My Thoughts on The Limits of Privacy Post 9/11

The conflict between privacy versus security has been a long-standing issue. A quote from Charles Fried gives a definition of privacy, "...one has privacy if and only if one has control over information about oneself" [3]. The meaning of privacy changes throughout cultures, and has become a significant issue in the digital culture, where it has become very convoluted. It is an issue that has ebbed and flowed as the result of events like the creation of the Patriot Act. The implementation of the bill changed privacy on the web in an unprecedented way. So what has privacy become?

The events of 9/11 were a traumatic event in the history of our nation, and the repercussions of our nation's response in the form of new laws are still felt today. The primary bill, in the context of this paper, is the Patriot Act. The bill put into effect a slew of laws that changed our country's concept of privacy and security in both the digital and analog worlds. Privacy means something different for every individual, but Fried's quote is the basic definition of what I believe privacy to be. My perspective regarding privacy is more geared towards confidentiality rather than transparency (which I also refer to as privacy versus security). Throughout my life, I have always had an introverted personality type. Whenever possible I try to keep as much of my personal information as hidden as possible. For this reason, I disagree with most of Amitai Etzioni's opinions in his book *The Limits of Privacy* who has, in general, the opposing opinion.

The conflict between the right to privacy and the right to security is the overall theme that is discussed in Etzioni's book. Etzioni discusses various topics that shed light on this conflict, both in the digital and analog realms. Some of the topics he discusses are testing infants for HIV/AIDS, rights of sex offenders, and encrypted messages. Etzioni's stance is that privacy should be protected until it becomes a problem for the "common good". He believes granting power to an authority like a government is necessary to maintain this balance between privacy and safety. While I understand his viewpoints, I generally disagree with his messages throughout the book. The term he uses "common good" is understandable, but also quite vague. This ambiguous term, I believe, could give entirely too much authority to a governing entity. The Patriot Act was established with the headline of protecting U.S. citizens, but the bill also infringed thoroughly on the right to privacy of citizens. This historical event, and the implementations of it, has driven my opinion of disagreement with Etzioni.

Etzioni's opinion about HIV testing for infants is one of only a few of his opinions that I agree with. I believe that is ethical to test infants for the presence of HIV/AIDS in their system and log that information in their medical records. I believe that determining whether or not an infant has HIV is beneficial because the infant can receive treatment and have a better quality of life. The downside of the determining this information is that as the infant matures, they can be forced into expensive health care premiums. Although it should be illegal, they may also receive some negatively biased behavior in their lifetime. My life experiences definitely influence this opinion. My family is financially secure, and thankfully no one in my immediate family has had any long-term medical

issues that would lead to expensive health care premiums. Perhaps if I had a different family life, I would feel differently about the issue.

Etzioni also discusses Universal Identification Systems and biometric scanning tools explaining that is an advocate for the technologies. He claims their implementation would be so beneficial to security and authentication systems that their constraints on privacy are an acceptable loss. I do not agree with this stance. I believe their use would infringe too heavily on users' privacy. I am a strong advocate for the right to anonymity, especially on the web. However, I do acknowledge that technologies like this will eventually become more prominent as we shift from Web 2.0 to Web 3.0. Web 2.0, as I am using it for this argument, is interacting with the web using profiles and input devices like keyboards. These profiles are a representation of users using written descriptions and images. In Web 3.0, we will represent ourselves using avatars. Avatars will be drastically more detailed in complexity and we will be interacting with these avatars using new input methods like Augmented Reality. This shift to Web 3.0 will require more intricate authentication methods to verify the complex avatars. In the future, I would be more willing to accept Etzioni's opinion, but for now his stance is too draconian.

Etzioni's stance on message encryption is another area in which I do not agree with. Data encryption using public and private keys to send private messages is a technology that is nearly impossible to break. Etzioni believes that for the overall security of the nation, the government should have the ability to access any message using a universal "master" key. I don't believe it would be in the interest of users to allow such overwhelming access to private information. Etzioni's argument also fails to mention the

scope in which the government could access messages. I don't believe it would be ethical for the government to screen every single message that passes through the major Internet hubs in the United States. I believe this is a major breach of privacy, especially if the sender and recipient are unaware of it. A message intended to be private should not be accessible by anyone other than the sender and recipient, regardless of the content of the message. In issues of this nature, I tend to fall back on the childhood concept of a diary. I think it is unethical for anyone besides the owner to view the contents of a diary. I realize that these two concepts are not entirely similar, but they still provoke the same psychological response in me; private messages should stay private. The potential assets of the technology in terms of national security would be a great benefit, but at far too high of a cost to the privacy of users.

Another book that discusses the developing issues of privacy on the web is *Click* by Bill Tancer. His book talks about the trends that have begun to emerge in digital world. Tancer talks about his career experiences as he saw very modern issues in regard to privacy. He talks about processes that go into harvesting data about large numbers of Internet users. The data harvesting company that provides the statistics that support Tancer's opinion is Hitwise. From Tancer's description, the companies try to harvest as little private information as possible to harvest their data. However, even when trying to avoid collecting sensitive information, some will slip through the cracks. I do agree with the ideology of the company, but it seems difficult to maintain.

Some of the important, and controversial, topics that Tancer's writes about in his book are porn, depression, and television on the Internet. Tancer's reports various

statistics in each of these topics, along with many others. The level of detail in these statistics despite the very large sample speaks volumes about how the data can be used. Tancer claims that the harvesting company Hitwise strips personal and private information from their harvesting, but do they really? What about the entities that exist to only do that. With the level of transparency on the Internet, how possible is it to stop entities with malicious intent from tracking users? It seems many of the technologies that we have created and utilized during the expansion of the Internet have greatly increased the risk to user privacy. For example, Cookies. Cookies allow users to stay logged into a website without have to re-authenticate after changing web pages, but cookies are also capable of holding private information in a very insecure way. They are also used as tools for tracking users by advertising companies, and other entities, frequently without user consent. A quote from an article analyzing the modern usage of cookies report, "... we observed that Facebook has the ability to track all users that have visited facebook.com at least once, and logging out from the service does not help users to avoid being tracked" [5]. The clear disregard for user privacy on the Internet makes me a strong advocate for privacy and anonymity.

I am a firm supporter of privacy and anonymity, but it seems many users on the Internet are not. Websites like Facebook are a prime example of this. Users of the website submit constant streams of personal information to share with their friends and family through the site. The privacy policies of sites like this state that they protect users' personal information, but what they say and how the act are very conflicting. Facebook has been the source of many privacy issues. A survey conducted by researchers

Besmer and Lipford found that, "... results indicate that Facebook users are not truly understanding and consenting to the risks of apps maliciously harvesting profile information" [4]. The term "apps" means third-party applications that run inside the Facebook network. It seems like many users aren't aware of these policies, or they simply don't care; I find this extremely disappointing. As the Internet will inevitably continue to grow, policies regarding privacy will become even more of a pronounced issue. I believe that the majority of users on the Internet, especially the increasingly large portion of younger kids, will need to learn about these issues.

As the digital realm continues to grow everyday, data that is on the Internet is becoming centralized. Websites are pooling massive amounts of data into singular points. Some of the types of data that are being centralized include medical records, financial records, and even social records. Facebook has over a billion monthly users who send a constant stream of personal information to the company's servers [6]. Massive companies like Google and Amazon have built data centers that hold hundreds of thousand of servers. These data centers provide a service known as Cloud Computing, which is essentially the remote storage of data. Data centers will eventually become the hosting grounds for everything from businesses to school projects. However, laws regarding privacy and security for theses data centers have yet to catch up to this emerging technology. Ferreira and Domingos explain that, "The undue access or unauthorized disclosure of private data kept in Storage Clouds has been referred as a critical problem, not only in the use case of secure data backup but also to preserve security guarantees of data accessed by online applications" [8]. I believe that laws

defining data protection in these data centers should be mainly geared towards privacy and security, rather than attributes like ease of maintenance. With only a single point of failure, any fault in network security could mean a substantial loss of private data. This issue will develop as we continue to move towards Cloud Computing.

The Patriot Act is a major issue for the United States, but privacy is an issue that affects cultures across the world. However, globalization has made issues involving privacy more transparent for the rest of the world. Areas like Australia are constantly facing similar issues where the Australian government is trying to balance privacy and security. The office of the Australian Information Commissioner have created an array of privacy principles to be followed by companies and organizations in Australia. The principles are, in general, geared heavily towards protection of privacy. For example, here is a section from the Information Privacy Principles under the Privacy Act 1988,

> Principle 1 - Manner and purpose of collection of personal information
>
> 1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
>
> (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
>
> (b) the collection of the information is necessary for or directly related to that purpose.

While these principles were written in an analog time period, the principles are still applied in the digital realm. Another area of the world that consistently deals with issues regarding privacy is Western Europe. The European Union (EU) have a “Digital

Agenda” which resembles the Australian Information Privacy Principles. The EU seem to have a firm ideology of protecting privacy, as demonstrated by a legal battle between the EU and Google in early 2013. A reporter discussing the controversy states that, “While Europe has some of the strongest data protection and privacy laws in the world, the U.S. doesn't” [10]. Even at a national level, values of privacy can change drastically.

Concepts of privacy differ from nation to nation as well as person to person. Opinions about the Internet and the privacy laws that influence can also differ between generations. Generations of people that lived in an analog world might have completely different opinions than someone who was born into the the digital. Younger generations are more comfortable using technology, whereas older generations might not be. A quote from a group of researchers Buhler, Neustaedter, and Hillman report that, “For many adolescents, connection with friends for socialization, relationship-building, and ‘hanging out’ now takes place online” [12,13]. This social medium did not exist 30 years ago, but it is almost an expected technology and skill for younger generations to use. On the other hand my parents still struggle with, as I see them, simple tasks like installing an application or navigating web pages. I’ve given both of them countless demonstrations and guides for interacting with computers, but it never seems to stick. They’ve even told me that they don’t have an interest in learning to use it because “it’s too late” for them. I believe it is this anxiety, fear, or resistance to accept new technologies that has created the divide between the generations.

There also seems to be a general lack of understanding of the consequences of using the Internet. The older generation seems unaware of the issue of privacy, while the

younger generation seems not to care. Again, I have personally seen both of these scenarios take place in my family. My father is far too willing to supply personal information to websites and is a sucker for advertisements; the same thing goes for my younger cousins. This demonstrates to me a lack of education about, what I will call, defensive web surfing.

The concept of privacy is interpreted differently by everyone. Each person, community, or nation has their own experiences and opinions that define their perspective. My personal opinion of privacy is that is should be held as a paramount ideology and should rarely being infringed upon. My opinion has been heavily shaped by the events I have seen in my life like the creation and implementation of the Patriot Act. This piece of legislation redefined the meaning of privacy in our country, both in the analog and digital world. The bill coincides with Etzioni's opinion that the security of the common good is more important than the right to privacy. I disagree with both Etzioni and the Patriot Act. Tancer's book which details the process of harvesting massive amounts of user data provide me with yet another reason to prioritize privacy over security. My concept of privacy is also driven by my personality traits, primarily by my introversion. I prefer whenever possible to share as little about myself, especially on the Internet. New technologies will continue to emerge and issues of privacy will emerge in parallel. However, as I continue to grow older I believe I will continue to hold onto my beliefs. These have been my thoughts about privacy.

References

[1] Etzioni, Amitai. (2000). *The Limits of Privacy*. New York: Basic Books, A Member of the Perseus Books Group.

[2] Tancer, Bill. (2008). *Click – What millions of people are doing online and why it matters*. New York: Hyperion.

[3] Fried, C., (1984). *Privacy*. In F.D. Schoeman (Ed.) Philosophical Dimensions of Privacy. New York, NY, Cambridge University Press.

[4] Besmer, A. & Lipford, H. (2010). *Users' (Mis)conceptions of Social Applications*. In Proc. GI 2010, ACM Press, 63-70.

[5] Chaabane, A., Kaafar, M. A., & Boreli, R. (2012). Big friend is watching you: analyzing online social networks tracking capabilities. *Proceedings of the 2012 ACM workshop on Workshop on online social networks*. 7-12. ACM New York, NY, USA.

[6] Tam, D. (2013). *Facebook by the numbers: 1.06 billion monthly active users*. http://news.cnet.com/8301-1023_3-57566550-93/facebook-by-the-numbers-1.06-billion-monthly-active-users/

[7] Privacy Rights Clearinghouse. (2013). *Chronology of data breaches*. http://www.privacyrights.org/data-breach.

[8] Ferreira, B., & Domingos, H. (2012). Management and search of private data on storage clouds. *Proceedings of the Workshop on Secure and Dependable Middleware for Cloud Monitoring and Management. Article No. 4*.

[9] Australian Information Commissioner. (2013). http://www.privacy.gov.au/index.php

[10] Whittaker, S. (2013). *Google's European conundrum: When does privacy mean censorship?* http://news.cnet.com/8301-1009_3-57571966-83/googles-european-conundrum-when-does-privacy-mean-censorship/

[11] Boyd, D. (2007). *Why Youth (Heart) Social Network Sites: The Role of Networked Publics*. Buckingham, D. (Ed), MacArthur Foundation Series on Digital

Learning, MIT Press.

[12] Marwick, A.E., Murgia-Diaz, D., & Palfrey, J. (2010). Youth, Privacy, and Reputation. *Berkman Center Research Publication*, No. 2010-5, 4-65.

[13] Buhler, T., Neustaedter, C., & Hillman, S. (2013) How and Why Teenages use Video Chat. *CSCW '13 Proceedings of the 2013 conference on Computer supported cooperative work*. pg 759-768. ACM New York, NY, USA.