The Criminal Impacts of Media on Privacy

Sophia I. Ripley

South Lyon High School

October 2017

Abstract

One's privacy is being invaded due to new media innovations. "From 2009 to 2013, the number of reported invasions of U.S. military or federal government computers jumped from 26,942 to 46,605, according to the U.S. Computer Emergency Readiness Team. That's not attempts. That's successes. How long before one of those shuts down a vital system?" (Maney, 2015, p.2). This stat speaks volumes of the risk the world is facing due to cybercrime. I specifically looked at the way people's privacy is at risk due to cyber criminals at work and government agencies trying to track down these crooks by having to act like one. The information collected has shown that the government has been in the shadow of these criminals: the government has been falling behind while this new generation of criminals continue to perfect their craft. People's privacy is in the crosshairs between the villain behind their screen and the federal agent behind their screen.

Keywords: cybercrime, hackers, privacy, media, and crime

The Criminal Impacts of Media on our Privacy

Riding a bike is a goal that every child had to work on and perfect. A child would get on their bike and even though they kept falling, that child would keep getting back on their bike every single time. This never give up attitude is the outlook ingrained in the mentality of every hacker behind a screen. People should now be more concerned with personal information put on the web due to these hackers constantly invading other's privacy. Also, these criminals have always been a concern of the government, but the hackers today have been gaining the attention of the government more and more as technology increasingly becomes a part of everyday life even more. As a result, the government must act like a hacker to track down these hackers. According to the former director of the CIA, "It's a new class of weapon -- a weapon never used before" (Maney, 2015, p.1). New media innovations have negatively impacted our right to privacy due to an increase in cybercrime and governmental involvement in catching these criminals.

Cybercrime and Criminals

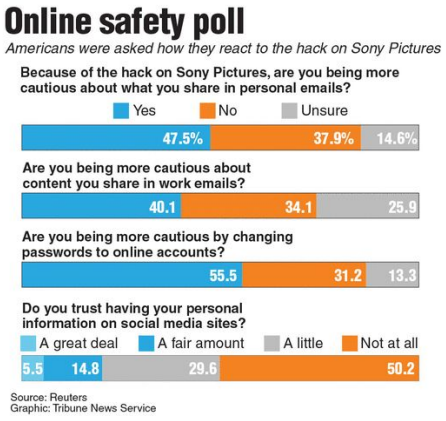
Crime has always been an issue for nations, organizations, and people in general. Now, with major improvements in media and technology, these new devices are just another way criminals intrude into one's privacy and personal life. Everyone is a possible victim to these cybercriminals, from businesses to government agencies, but in the end the individual is always the one affected the most. For example, when the FBI busted a Milwaukee group of hackers that go by the name 414s, they discovered that the group was responsible for breaking into 60 computers, such as the Los Alamos National Laboratory (Trigaux, 1998). These sixty computers belonged to sixty groups with millions of workers; the effects of these hacks also spread to the families of the workers. In addition, another example of cybercriminal activity is when the federal government took down:

> "Carlos Felipe Salgado Jr. known online as 'Smak.' Salgado was caught last year after stealing 10,000 credit card numbers off the files of an Internet service provider in California. Salgado then tried to sell them for $260,000 to an undercover FBI agent." (Trigaux, 1998, p.4)

"Smak" only had 10,000 credit cards this time which equal up to 10,000 lives nearly sold away. It is important to also think about the amount of credit cards and lives he had in possession before this bust, too, and how many victims were involved.

Out of all the hacks, the one that shocked the world was the Sony hack in April of 2011. "Although information stored on the network was supposed to be off-limits to outsiders, someone had found a way to access this data online...and Sony...admitted that the data the perpetrator had viewed… included customer credit card numbers...bill addresses and birth dates" (Currie, 2012, p.24). This was a devastating attack to many Americans because they have never seen a security breach like this before. As a result, many Americans started to take a lot more precautions when dealing with the web as shown by the graphic below.

Visual 1: Online Safety Poll - Americans were asked how they react to the hack on Sony Pictures



As seen by the graphic, roughly 50% of people still don't trust putting personal information out there on social media and close to 55% are now changing their passwords to their online accounts due to

this attack (Maney, 2015). Also according to Maney, roughly 47% are becoming more cautious of what they share on their personal email and about 40% are concerned about the content shared in their work emails (2015). This attack made many people concerned about cyberthieves, especially when it came to privacy and the leakage of personal information. These cyberthieves are only looking out for the betterment of themselves and clearly not the other person getting scammed. People should become more attentive to what personal information is on their device.

Cybercriminals steal items such as credit card numbers, social security identifiers, and much more. These criminals then sell the private information for a profit. For example, they might sell a single credit card for $10-$20 and a social security number for $50 (Currie, 2012). Many of these crooks don't evaluate the effects of their actions because selling an item like one's social security number is like selling one's life away. An individual's privacy is wrecked and this criminal activity ruins one's life. In fact, some cybercriminals, like the Sony hackers, are more interested in the items that are more devastating if placed in the wrong hands, these include birth dates, social security numbers, and driver's license numbers (Currie, 2012). Furthermore, the end goal of all cyberthieves is to become an identity theft, which is huge nowadays. Latanya Sweeney, an Internet safety expert, says in order to apply for a credit card, all one needs is their name, social security number, birthdate, and address. These cybercriminals can easily obtain all of this private information due to their digging and stealing of personal information through today's technology. Many might say that the chance of getting hacked and their privacy being invaded by these cyberthieves are slim, however, "according to one study, about 10 percent of Americans have been victimized by identity thieves, and information theft affects approximately 10 million Americans in any given year (Currie, 2012, p.25). This type of criminal does pose a sufficient threat to an individual's privacy and does all of this damage simply by hiding behind a screen.

Government Control

Not only have new innovations in technology upgraded the average person's life, but advanced media has also impacted and improved the federal government's life. Before, the U.S. federal government was left in the shadows of these cybercriminals that would send federal agencies down a never ending path of code and encryption. However, certain laws with loopholes and specific tools make the federal government's job easier to track down these criminals. The issue though, is that the federal government could be looking into one's personal information without the individual even knowing it, as a result, upsetting one's privacy.

9/11 was a major turning point in American history and made Americans vigilant. A major law put into place in order to prevent future attacks from occurring is The USA Patriot Act. This law gives the federal government access to personal information and was passed with a unanimous vote in Congress following the terror attacks of September 11th. The original plan for the act was "to monitor people's activities without their knowledge" and to shut down a possible terrorist operation (Currie, 2012, p. 21). The law not only expanded the federal government's ability to record and listen in on private phone calls using a tool called "the pen register" (O'Neil, 2001, p.3), but the law also gave federal agents access to a suspect's Internet records (Currie, 2012). According to Currie on page 21, "The FBI can ask Internet service providers to turn over a log of the web sites a person visits and the addresses of email coming to and from the person's computer" (2012).

Another act that deals with the federal government's motives is the Electronic Communications Privacy Act of 1986 which allows the federal government to have access to emails. According to O'Neil, this act is, "a key weapon in the government's arsenal against computer crime" (2001, p.3). At this time, many Americans probably didn't really understand the depth of this act since technology was progressing slowly. However now, in the 21th Century where technology seems to control every aspect of human life, this act, coupled with The USA Patriot Act, are a dynamic duo that pries into individuals' lives everyday

in hopes of shutting down any criminal operations. In regards to these acts, many people often contemplate whether one's privacy is being invaded for the common good of America.

Another key law that gives the federal government some "wiggle room" to track down an individual down is the Privacy Act of 1974. This act "limits the amount of private information government agencies may share with one another" (Currie, 2012, p.22). To demonstrate, Currie states that on page 22 , "it is against the law for the Census Bureau to give personally identifiable information about an individual to any other individual or agency until 72 years after it is collected" (2012). The fault in this law is that a federal agency can share this exclusive information to other groups or private companies.

This issue is not only an issue at the federal level, but this situation is starting to become present at the state level, too. According to Currie, about $13 million is made each year in Oklahoma due to Oklahomans' private information being sold to attorneys, insurance companies, and other individuals (2012). Furthermore, the government can pass this information, such as driver's information, onto buyer after buyer with no knowledge of the buyer's reliability (Currie, 2012). This is a startling fact and a major concern in that one's personal information can end up in the wrong hands and one's privacy would be invaded. Ultimately, one can become a victim of identity theft.

Another major tool used by the federal government is called "Carnivore" (O'Neil, 2001). This "new Internet sniffing device" that monitors the web, "selects and stores communications the government is authorized to intercept," like an Internet address (O'Neil, 2001, p.3). The troubling news is that Carnivore is controlled by the federal government. This programs also gives the federal government an excessive amount of power and control compared to the old system named Ma Bell (O'Neil, 2001). In fact, the attorney general recently ordered an investigation done by a major university (O'Neil, 2001) and saw that the idea of privacy is not so black and white anymore in this digital age. Not only does Carnivore mess with one's privacy but, it also messes with the checks of powers in the federal government.

In addition, this is not only a problem in the United States. The European government also has a similar system in place called Enfopol 98, and soon, DNA databases that will provide everything under an individual's name by only scanning a fingerprint (Davies, 2001).

The scary thought is these are only a few of the tools and laws that help the federal government track down criminals. Many of these laws and tools bring up the controversial topic of privacy and whether the line is being crossed or not. Debates in Congress have sparked reform when it comes to this topic of fighting the war on cybercrime, however, these new ideas will takes years and years to fix the system in place. Talks about possibly adding a "Department of Cybersecurity" to the president's cabinet has been discussed but seems very unlikely (Cohen and Evangelakos, 2017). Also, plans to allocate more resources for cybercrime investigations are in store for the future, but with these resources come more power for the government. Congress has discussed focusing on the individual's privacy rights in the digital world, too, and hopes to pass laws regarding this topic. However, these talks are very vague and no actual plans seems to be in place, just a bunch of chatter of hopes and dreams. The truth is the federal government doesn't seem to know how to balance its responsibilities of catching criminals and trying not to invade one's privacy. These ideas sound great, but the question that remains is whether or not the federal government is really going to step in and protect what the Founding Fathers fought for?

Through my research, I have discovered that both cybercriminals and the government have a role in invading people's privacy. Now, people need to learn to be more vigilant of these cybercriminals and become aware that the government could be looking into one's personal information, if one has committed a crime. There is a famous quote by Christian Lous Lange that says, "Technology is a useful servant but a dangerous master." Technology is rapidly evolving and people must consider the personal information that is put out on the web, and the possibility of one's privacy being taken away. One must

learn to master the system and have that never give up attitude, just like riding a bike, when facing the villain.

References

Cohen, R. H., & Evangelakos, J. (2017, 12 Jul). America isn't ready for a 'cyber 9/11'. *Wall Street Journal* Retrieved from https://sks.sirs.com/webapp/article?artno=395795&type=ART

Currie, S. (2012). *Issues in the digital age: Online privacy* Issues in the Digital Age: Online Privacy. Retrieved from https://sks.sirs.com/webapp/article?artno=0000393944&type=ART

Davies, S. (2001, Mar). The spy in your refrigerator.. *UNESCO Courier (United Nations Educational, Scientific, and Cultural Organization)*, 18+. Retrieved from https://sks.sirs.com/webapp/article?artno=0000133285&type=ART

Maney, K. (2015, Jan). Sony was just the beginning. *Newsweek,* Retrieved from https://sks.sirs.com/webapp/article?artno=0000370363&type=ART

O'Neil, M. (2001, Cybercrime dilemma. *Brookings Review,* , 28-31. Retrieved from https://sks.sirs.com/webapp/article?artno=0000133248&type=ART

Trigaux, R. (1998, 14 Jun). Hackers: The underbelly of cyberspace. *St.Petersburg Times*

(St.Petersburg, FL) Retrieved from

https://sks.sirs.com/webapp/article?artno=0000023027&type=ART