Cybercrime: Our Lack of Privacy

Hunter Elandt

South Lyon High School

December 2017

Abstract

This paper's main focus is to evaluate the increase in cybercrime over the years and how that has affected our privacy. Since the introduction of the first social networking site in 1996, new innovations in media technology have rapidly changed our world; However, along with these came many new weaknesses for us to cybercrime. The amount of cyber attacks has tripled in the last decade, and will continue to gradually increase as we move forward. While doing my research, there were 4 main topics I focused on: The different forms of cybercrime, the increase in privacy protection, government intervention, and looking to the future. I felt that these topics were most beneficial to my claim, and also provided a very large amount of information to go off of. Focusing on these main 4 allowed me to narrow my research down, which made it much easier to not only find sources, but to find quality sources with quality information. While finding my sources, I made sure that all my information was relevant to the overarching prompt of privacy. As a result, I found that while new innovations in media technology are drastically changing the way we live and making our lives easier, we are becoming increasingly susceptible to criminal activity over the web, and new forms of privacy control are constantly being put into the works. In the end, my research is devoted to exploring in-depth how even though new media technologies are good for us, they drastically decrease our privacy and put us at a higher risk to encounter cyber criminal activity.

Word Count: 262

Introduction

Privacy is everything to us. Whether it's in public or online, our privacy is number 1. This becomes a concern then when it comes to new media innovations. Such things as the internet and especially social media are rapidly changing the way we live and go about our daily lives. We are able to connect and meet people that we never would have even dreamed of meeting in years past, and we can find out about huge events happening around the world simply by the click of a button; However, with these comes a huge downfall. Cybercrime. Cybercrime is criminal activity performed by a computer or over the internet, and with the introduction of these new media technologies, we have in turn made ourselves more susceptible to this. New forms have been discovered in the last few years, which has lead to the need for on increase privacy protection laws, along with the government intervening to attempt to catch cyber criminals. As we move forward into the future, how we define privacy online will continue to change and shape the way we go about using the internet forever.

The Different Forms of Crime

Along with the new innovations in technology came new innovations in cyber crime. Hackings have evolved into accounts being taken over, financial information being digitally stolen, etc. There are two major forms that have come into the light full force over the last few years. These include spam emails and spyware. Everyone knows what classic spam emails are. They are the annoying emails you receive over and over again from a business or a group; However, some of these can have a very **ominus** intentions. Behind spam emails can be malicious viruses that are intended to harm your computer or steal your information. Such viruses include, malware, trojan horse viruses, and many more. Spam has actually become one of the top modes for transmitting viruses, and according to Westin (2017), spam will continue to pose a growing threat to online privacy in the future. Spyware is the other form of crime that I mentioned. This can either be very harmful or not at all. “Frequently installed without a user’s knowledge or permission, spyware programs may monitor and report all internet activity to a remote observer (Westin, 2017, para. 12). This observer can be anyone. It can be an advertiser simply looking to display their product to you on the websites you commonly visit, or it can be a hacker, looking to gain complete access to your computer and all your personal information. Yes this can occur. Usually it is used with a trojan horse program, and when it is, someone can completely breach your computer. This is very concerning, as according to Westin (2017), 90% of computers had some sort of spyware by 2004. It is completely unknown whether either spam or spyware is harmful when you experience it, as it can be either or. Knowing this, does it seem worth it that these new media innovations basically create a new open door for cyber crime?

The Increase in Privacy Protection

As the public became away of the increasing levels of criminal activity online, concerns for their privacy skyrocketed. More advanced computers came into play, and which rallied millions more into the use of them. This mass use created online databases of information that anyone could access. This became a concern. Another concern that arose was that with the new innovations in telephones and cell phone, people were afraid of their calls being intercepted and information being stolen by hackers. This concern grew and grew and eventually politicians began using this as a campaigning tool. “ First, privacy became a bipartisan issue, with both Democratic and

Republican leaders advocating new privacy-protection laws (Westin, 2017, para. 19). The concern continued to grow from there until finally congress decided to do something about it. New privacy laws were enacted from 1996-2000 that put rules on electronically transmitted health information and financial service firms (Westin, 2017). This was the first round of privacy laws that we received. Since then, many more have be enacted, which brings us to the next point. The government.

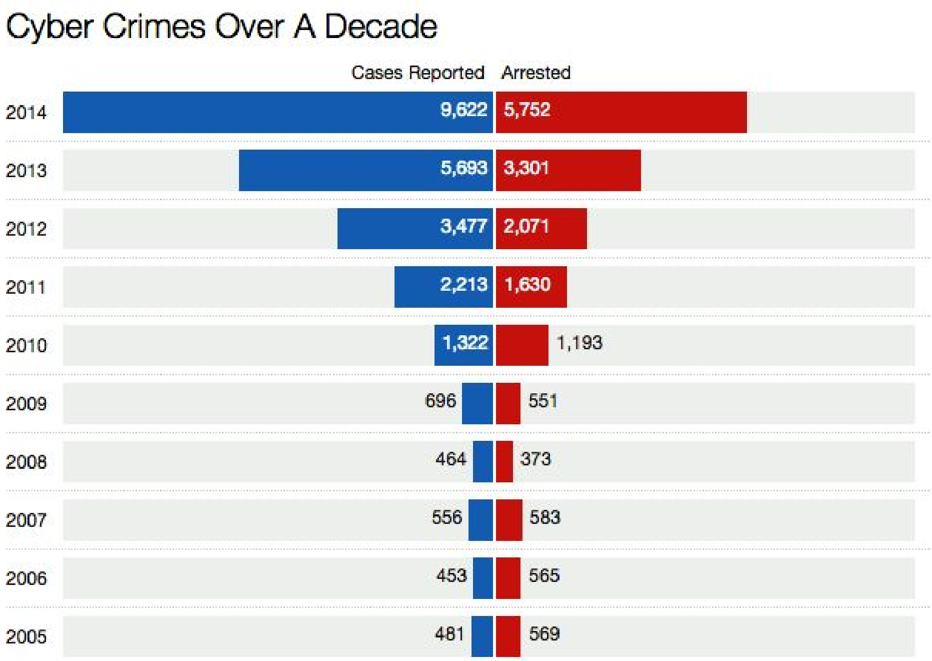
Government Intervention

When the privacy crisis hit, the government was quick to pass laws and acts that worked to input rules and restrictions on online activity. Along with this, they took a hard shot at cyber crime. After the September 11 terrorist attacks, security really stepped it up, and new programs to catch online criminals were put into action. The government began using a system called Carnivore, which allowed them to detect the destination of criminal activity over the internet (Levinson, 2017). This and many more were included in a bill added to the Patriot Act, which was put in place to fight against terrorism. When the public found out about Carnivore, major concern arose again as people feared that this program allowed the government to not only detect criminals, but detect anyone, and track what they did on the web. This led to the discontinuation of Carnivore in 2005, and from there they switched to more “available” needs. The NSA began wiretapping without warrants, and “It opted for commercial spyware programs and paying internet service provider (ISPs) for their cooperation in tracing suspicious internet activity” (Levinson, 2017, para. 10). These spyware programs included Key Escrow, and Magic Lantern. Key Escrow gave the government the ability to decrypt any encrypted transmissions they intercepted, and Magic Lantern made it possible to monitor anything typed into someone's computer. This again raised concern with the public. See a pattern here? People were still under the assumption that the government was **concocting** some sort of plan in order to monitor not just criminals, but everyone. Despite these accusations, the government still claims that all these programs are used to prevent cyber criminal activity and protect the people.

The Future

As it stands, if we continue in the direction we're headed, cybercrime is only going to continue becoming more of a problem. "Technological advances have made necessary further definition of privacy" (Levinson, 2017, para. 12). Social media sites have become very popular in recent years, and have they have not helped in minimizing the issue. Sixdegrees.com was the very first social media site introduced in 1997. It did what most sites do now: make a profile, upload pictures, add people as friends and send friend requests to others, and share information. This led to the invention of many sites that are still around, including Facebook, Twitter, etc. These sites try to maintain the privacy of their users, such as giving the option to make your account private, or reminding you to **abstain** from posting personal information, but it is simply not enough.

Figure 1- Cyber Crime over the Decades. This figure shows the increase in cybercrime cases reported and arrests made from 2005-2014.



As you can see by this graph, the cases of cyber crime reported in a span of 10 years increased by over 9,000! That is an absolutely absurd number, and we have new media technology to blame for it. Like I said, social media has changed our lives forever, but with numbers like these, it is imperative that privacy be our number one concern when it comes to our internet use. (Levinson, 2017)

Conclusion

As it stands, we will continue to improve technology as fast as we can and progress forward into the future. “Clearly, there are privacy concerns in this socially networked world. But, for now, interest has not slowed” (Social Media, 2017, para. 19). People will continue to be interested in new media technologies despite the fact that they make us more susceptible to cybercrime. If we continue down the road of showing little care for our privacy, the online future doesn’t seem very bright.

References

1. Levinson, S. (2017). Privacy, Invasion of. *Grolier Multimedia Encyclopedia.* Retrieved November 13, 2017, from Scholastic Grolier Online. http://gme.grolier.com/article?assetid=0236265-0
2. Westin, A. F. (2017). Computers and Privacy. *Grolier Multimedia Encyclopedia.* Retrieved November 13, 2017, from Scholastic Grolier Online. http://gme.grolier.com/article?assetid=0069282-0
3. Social Networking. (2017). *Grolier Multimedia Encyclopedia.* Retrieved November 13, 2017, from Scholastic Grolier Online. http://gme.grolier.com/article?assetid=10004873
4. Social Media. (2017). *The New Book of Knowledge.* Retrieved November 13, 2017, from Scholastic Grolier Online. http://nbk.grolier.com/ncpage?tn=/encyc/article.html&id=10537389&type=0ta
5. Tebbel, J. (2017). United States of America: Media. *Encyclopedia Americana.* Retrieved November 13, 2017, from Scholastic Grolier Online. http://ea.grolier.com/article?id=0432913-00
6. Venkataramakrishnan, R., Katakam, A., Chari, M., Conversation, R. M., Sudevan, P., Kirpal , N., & D'Cunha, Z. (216, June 03). As internet use spreads, cyber crimes rise 19 times over 10 years. Retrieved December 07, 2017, from http://scroll.in/