Shu Ying Lin

Professor Gladson

ENGL 102

9 December 2018

Minimizing Risks of Invasion of Privacy

In order to receive a better and a more personalized online experience, allowing service providers to have access to personal information is not uncommon. However, having access to one's personal information does not always mean having the ownership of it. Sharing individual's personal information without having his or her consent can be considered an invasion of privacy. The social media giant Facebook has learned its lesson back in March 2018. The Facebook-Cambridge Analytica data breach has cost Facebook significantly as well as compromising millions of Facebook users' privacy (Badshah). By giving incentives to users who agreed to share their data, an app affiliated with Cambridge Analytica was able to collect both users and their friends' information (Badshah). The personal data collected by Cambridge Analytica were analyzed and used to secretly assist the Donald Trump presidential campaign in the United States presidential election of 2016 (Badshah). In this political scandal, Facebook users' data were used on a purpose beyond what users originally consented to. Not only is what the users experienced an invasion of privacy, it is also a potential starting point of more data security issues.

The Facebook-Cambridge Analytica data breach political scandal shows the destined vulnerability of online personal data regardless of users' awareness about data security. Even non-users of the app might still be impacted by the incident if they are friends of the app users. About nine months before the scandal attracted a large amount of media attention, Facebook

Newsroom announced that the number of monthly active users had reached two billion (Nowak and Spiller). Given the fact that Facebook is not a small business but a multi-billion dollar social networking service company, it must have a number of employees who specialize in cybersecurity and are capable of recognizing suspicious activities. This world-famous incident shows that whether there is a group of computer science experts or not, there can often be a method for people with bad intentions to obtain and use certain information illegally. Online users' personal information is therefore left at a vulnerable position, and no one can guarantee absolute privacy of their data. These types of situation can lead to credit card fraud, email spam, and various types of identity theft, depending on the types of information stolen. Because data security is both a significant and inseparable part of today's digital age, the government and technology companies should act on their own initiatives to eliminate online users' data being misused, and Internet users, parents, and school should raise awareness of online privacy to minimize the potential risks of data breach.

The government being a victim of data breach is not new either. Data breach may threaten the status of a country in many ways, such as national security, financial situation, and reputation. According to the U.S. Office of Personnel Management, the background investigation records of about twenty-one million individuals were stolen in June 2015. Among the vast amount of stolen data, sensitive information including social security numbers were part of them. Because government agencies can also be victims of this type of incidents, the government should initiate appropriate actions by legislating stricter laws that are up-to-date to today's technological dynamic. The General Data Protection Regulation passed by the European Union is an example of how the European Union imposes restrictions on companies whose daily operations rely on users' data information. Though the European Union is not classified as a

government, it is able to influence the governments of its member countries. The main purpose of the law is to protect people's personal data from being misused by governments, companies, and other types of organizations (Ruth). By having such regulation, the government can help promote data security and raise awareness of dangers of not taking actions to protect personal information online. Certainly, it is unlikely to have just one set of laws or regulations that ends all cybercrimes as cybercriminals are able to find newer ways to disguise themselves and steal personal information on the Internet. Having laws with more serious consequences may deter skillful hackers from committing cybercrime even though cybercriminals might not be identified and caught every time. The existence of these laws may also help prevent disputes between the people and businesses.

In addition to government's effort to protect its citizens from identity theft, technology companies, particularly those who handle a massive volume of data on a daily basis, can also contribute to decreasing the rate of online users' data being used unauthorizedly. There are several reasons why technology companies should take users' privacy seriously. First, the use of online services by online users helps companies make money both directly and indirectly. Online users may choose to not use certain online services if they see that their sensitive data cannot be safely stored. Another reason is that being clear and transparent about how users' data are used may help improve a company's image and gain trust from more service users. In Neil Richards and Woodrow Hartzog's "Privacy's Trust Gap," they suggest that the increasing tendency of online users sharing their sensitive information online has made trust a more and more important aspect for large technology companies. As a result, it is crucial to have technology companies do more than just periodically inform their users about their terms and conditions, privacy policies, and how their users' data are actually being used. Most of the time, companies require some

personal information to be shared with them to provide more personalized services. Without the trust between those technology companies and their users, companies would be less likely to retain users and make profits with advertising to the appropriate audience. Protecting users' privacy is not only for the users' benefit but also the companies'. If the process of storing and analyzing users' data is not conducted securely and properly, skillful hackers with malicious intent might be able to obtain and use others' information illegally. Therefore, technology companies must be prepared to handle situations like this and provide relevant resources to their users. Facebook has started taking comprehensive actions to better protect its users' privacy by limiting app developers' ability to access certain data after the Facebook data breach scandal gained national attention (Deagon). If Facebook had done this as a pre-emptive action to protect its users data, perhaps Facebook's chief executive officer Mark Zuckerberg would not have to be in the congress and questioned by senators and representatives for hours. Facebook's negligence on the security of users' data prior to the incident and the shows the importance of technology companies taking initiatives on this matter.

Online users have an irreplaceable role in protecting their own data privacy because they are the people who decide what personal information to share. Simson Garfinkel who was an associate professor in California suggests in his article "Internet Privacy Can Be Protected" that the release of some aspects of personal information is inevitable in today's information age even if individuals choose not to use certain services. Invasion of privacy can be a result of not being proactive in protecting one's own personal information. According to a study mentioned in Mansour Alsaleh, Noura Alomar, and Abdulrahman Alarifi's research, over sixty-five percent of surveyed smartphone users have settings that pose risks to their data privacy on their phones despite being worried about their data being stolen. Given the fact that the result of the study

shows there are users who are willing to compromise their data privacy for services, online users should understand the risks of being online and using different types of services available online and be more aware of actions they can take to defend invasion of privacy. A lack of data security can lead to serious problems. Learning about data and privacy can benefit online users in several different ways regardless of whether or not they have been victims of data theft. Online users will less likely be a victim of invasion of online privacy if they are able to detect some common types of fraud techniques. On the other hand, victims of identity theft will know where to seek resources, be capable of taking actions against perpetrators, and have them face legal consequences. Therefore, it is best to have online users learn some basic knowledge of online privacy.

Along with the attention from the government, technology companies, and online users on online privacy, parents' involvement in promoting data security can help build a strong foundation of their children's knowledge of digital privacy. In the past decade, the Internet has become more accessible together with advancements in technology, such as Wi-Fi, smartphones, and tablets. This means that more families have computers and Internet access at home, which also means that children of today's and future generation may be exposed to the digital world from an early age. Children are generally less mature than adults and so they might have a higher chance of performing risky online behaviors that can potentially lead to identity theft. In Olesya Venger's study on readability of policies of online gaming environment specifically designed for children, Venger analyzes the readability of Neopets's both terms and condition and privacy policy using the Flesch Readability Index and Automated Readability Index. The scores of both policies indicate that the contents are very difficult to comprehend and are best understood by college students or graduates (Venger). The hard-to-read statements put young children and

teenagers at a disadvantage while they utilize different kinds of services online. Without having basic knowledge of data and privacy, children and youths are at higher risks of being victims of invasion of privacy. To protect children's privacy online, parents can first teach the importance of having privacy rights. Teaching children about online privacy raises their awareness of how they and others can be deeply affected if their right to privacy is violated. Letting parents give their children a lesson about online behavior and privacy is perhaps a slow yet the most effective method of minimizing the rate of individual's privacy being violated as parents typically have direct influence on their children. After all, it is easier to instill a sense of responsibility for their own privacy and moral values to their children while they are still young and innocent. One day in a society where they have all become adults, there will be fewer victims of identity theft and cybercriminals in the future.

The education about online behavior and privacy children receive at school also plays a significant role. Schools can better facilitate the discussion of online privacy among groups of students, which is something families are not able to do at home. According to a 2015 study conducted by Lenhart, there are "92% of teens report going online daily, with almost 25% reporting constant use of online resources" among two thousand survey respondents aged from thirteen to seventeen (qtd. in Guinta). Also, as young children get older, more start to use mobile devices to socialize with their peers (Dias-Fonseca). The two findings above show the necessity of learning online privacy at home and having them reinforce what they have already learn at home. It is especially important to expose this topic to students early as they gradually become involved in social media. Not being fully aware of how information posted on social media may be used can pose obstacles in these young social media users' and their peers' future. As suggested by Carrie James and other authors in "Young People, Ethics, and the New digital

media", "unwitting participants in the digital public may be the most frequent victims of privacy lapses." One's reputation and opportunity to succeed can be ruined if potential employers or college admission staff unintentionally see the individual's inappropriate photos and videos posted online by the individual's friend (James et al.). Reflecting back on the Facebook's scandal, the hypothetical situation proposed by James can be a reality. Being a victim of loss of privacy can be caused by the lack of online privacy awareness of the victim's friend or family, and it does not necessarily mean the victim has engaged in some online risky behaviors.

Some victims of data breach may argue that technology companies and organizations responsible for collecting users' data should take full responsibility of consequences of data breaches and invasion of privacy. Their point of view makes sense because they would not have to experience the negative impact of privacy loss if companies had not requested their personal data in the first place. However, they need to realize that the interests of the users and service providers are interconnected. Without either one, companies would not be making profits, and people would not have access to online services. Convenient or entertaining online services are developed and designed by companies to meet the needs of online users. Users' online habits are heavily based on the types of online services available for their needs. How will companies be able to provide quality services if they do not have basic knowledge of their intended users? In addition to the mutual relationship between Internet users and companies, invasion of privacy is sometimes a result of users performing high-risk online behavior on platforms provided by technology companies. To name a few risky online behaviors, they include sharing home address and telephone number online, sharing every aspect of one's life on social media, and clicking on suspicious unknown links posted by others. Therefore, technology companies should not bear all

responsibilities for users' risky online behaviors. Online users should learn about this issue as well to prevent their information being stolen by hackers.

To conclude, there are many ways to eliminate the irreversible effects of data breaches. Personal data can help businesses provide better personalized services to potential clients and customers and online users receive information that is useful and relevant to them. By demanding specific actions from the government, organizations with authority, and technology companies, both the people and businesses can achieve a win-win situation. Raising public awareness is just as important because people will know what to do when their right to privacy is violated. With so many different kinds of issues related to online privacy, it is best to raise every one's attention for the potential risks of being online and using online services and have different groups of people contribute to this matter to minimize all the potential risks of data breaches and invasion of privacy.

Works Cited

Badshah, Nadeem. “Facebook to Contact 87 Million Users Affected by Data Breach.” *The Guardian*, Guardian News and Media, 8 Apr. 2018, www.theguardian.com/technology/2018/apr/08/facebook-to-contact-the-87-million-users-affected-by-data-breach.

“Cybersecurity Resource Center Cybersecurity Incidents.” U.S. Office of Personnel Management, www.opm.gov/cybersecurity/cybersecurity-incidents/.

Deagon, Brian. “Mark Zuckerberg, The Facebook Data Breach And The Dark Side Of Social Media.” *Investors Business Daily*, 23 Mar. 2018, p. 11. EBSCOhost, search.ebscohost.com.montgomerycollege.idm.oclc.org/login.aspx?direct=true&db=bwh&AN=128647202&site=eds-live&scope=site.

Dias-Fonseca, Tania, and John Potter. "Media Education As a Strategy for Online Civic Participation in Portuguese Schools/La Educacion Mediatica Como Estrategia de Participacion Civica Ondine En Las Escuelas Portuguesas." *Comunicar*, vol. 24, no. 49, 2016, p. 9+. Expanded Academic ASAP,

Garfinkel, Simson. "Internet Privacy Can Be Protected." Privacy, edited by Roman Espejo, Greenhaven Press, 2010. Opposing Viewpoints. *Opposing Viewpoints in Context*, http://link.galegroup.com.montgomerycollege.idm.oclc.org/apps/doc/EJ3010434244/OVIC?u=rock77357&sid=OVIC&xid=1ba7a96d. Accessed 29 Nov. 2018. Originally published as "Privacy Requires Security, Not Abstinence: Protecting an Inalienable Right in the Age of Facebook," *Technology Review*, vol. 112, July-Aug. 2009, pp. 64-72.

Guinta, M. R., & John, R. M. (2018). Social Media and Adolescent Health. Pediatric Nursing, 44(4), 196-201. Retrieved from

https://montgomerycollege.idm.oclc.org/login?url=https://search-proquest-com.montgomerycollege.idm.oclc.org/docview/2096475619?accountid=39773

James, Carrie, et al. "Young People, Ethics, and the New Digital Media." *Contemporary Readings in Law and Social Justice*, vol. 2, no. 2, 2010, p. 215+. *Opposing Viewpoints in Context*, http://link.galegroup.com/apps/doc/A267134532/OVIC?u=rock77357&sid=OVIC&xid=8e9e2331.

Nowak, Mike, and Guillermo Spiller. “Two Billion People Coming Together on Facebook.” *Facebook Newsroom*, Facebook Newsroom, 27 June 2017, newsroom.fb.com/news/2017/06/two-billion-people-coming-together-on-facebook/.

Richards, Neil, and Woodrow Hartzog. “Privacy’s Trust Gap: A Review.” *Yale Law Journal*, vol. 126, no. 4, Feb. 2017, pp. 1180–1224. EBSCOhost, search.ebscohost.com.montgomerycollege.idm.oclc.org/login.aspx?direct=true&db=a9h&AN=121522304&site=eds-live&scope=site.

Ruth, Michael. “General Data Protection Regulation (GDPR) .” *Salem Press Encyclopedia*, 2017. EBSCOhost,search.ebscohost.com.montgomerycollege.idm.oclc.org/login.aspx?direct=true&db=ers&AN=125600230&site=eds-live&scope=site.

Venger, Olesya. “Internet Research in Online Environments for Children: Readability of Privacy and Terms of Use Policies; The Uses of (Non)Personal Data by Online Environments and Third-Party Advertisers.” *Journal of Virtual Worlds Research*, vol. 10, no. 1, Jan. 2017, pp. 1–15. EBSCOhost,search.ebscohost.com.montgomerycollege.idm.oclc.org/login.aspx?direct=true&db=ufh&AN=124007093&site=eds-live&scope=site.