Taking a Broader View of Responsibility on Privacy and Data Protection

Xuan Thanh Do 9/29/18

George Mason University IT 104-002

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Background

In the more recent decades of the information age, information technology as an industry has experienced continued growth as well as enormous transformations for businesses and consumers. Alongside the numerous positive impacts on society is a new development, an ongoing need, in data protection of personal information. When digital information is not firmly secure, new threats of identity theft, cyber attacks, and security breaches endanger the privacy of personal data. These accidents are grave; they threaten online privacy by stealing or exposing data and subjecting corporations as well as consumers to cyberattacks or misuse of personal information. Currently, data protection has become more and more relevant to the security concerns of large corporations and consumers with the general public. One social networking site in particular, Facebook, has come to the front lines of the "security arms race" (Matasakis & Lapowsky, 2018). With an election scandal and recent security issues, Facebook's mistakes demonstrate the importance of data protection and privacy. In recent events, Facebook has called on large technology corporations holding personal information to adopt more broad views of responsibility. Furthermore, the use of stronger levels of data privacy and more robust security practices ensure that there is a better standard of online data protection for individuals and companies relying on keeping data security measures up-to-date. Large technology companies like Facebook can establish a more marketable appeal that builds a foundation of trust for its users and consumers.

Within recent years, the expectation of society for progress in data security has become one that is reasonable and necessary : data privacy should be bound to consumer needs and expectations. Social marketing appeal is an addition to the Internet economy driven by social networking sites like Facebook and Twitter. Facebook's social media platform already allows businesses to promote new features of products and services for consumers. For instance, Apple advertises on Facebook the new updates that come to their operating system to allow consumers to be up to date on the newest uses, changes, and personalizations within their electronic devices. Furthermore, Apple is not the only multibillion dollar corporation to convey the upcoming changes for consumers before they are released to the market. Companies from large to small utilize social networking sites like Instagram and LinkedIn as a source of advertising and online presence. Even small start-up companies use online social media platforms to market their businesses to allow consumers to obtain their goods and services.

With all of the content and services from social networking given, security concerns arise when access within social networking sites is given to users upon agreeing to terms and conditions. Oftentime, the terms are not simple and overly complicated for most users. Upon agreement, social networking sites sell personal data to large advertisers and developers. In reality, very few users read their sophisticated terms of agreement, but they agree anyways. Users consent to allowing these sites to access their services, content, and platforms to communicate, share information, and/or promote business. Thus these sites have convinced users to give up ownership of their own personal data. Consenting blindly to these binding agreements online is a problem. When users are not educated or informed on how personal information is collected or processed, there are more opportunities for other parties to misuse their data. One challenge to security concerns is the misuse of data by large technology companies. The internet's business model depends on people sharing their personal data in exchange for access to content, services, and social media platforms. Therefore, Facebook makes money from you by selling your personal information to advertisers. Misuse of information stems from both actions taken by third parties who purchase personal data and the absence of being informed on privacy and data protection. Privacy concerns should be clearly detailed and readily addressed by companies when access is given to individual users. Privacy agreements outlines conditions that allow users both identity and autonomy that are within the scope of appropriate usage and behavior. Data protection is more specific term that underlies laws, policies and regulations of how data is handled. The laws and regulations referenced are concerned with the ways third parties interact with the information that they hold about us; how data is collected, processed, shared, stored, or used, and most importantly if it is handled with or without consent.

Misuse of information can take on many different manifestations. In 2016 Facebook was involved in an election scandal, “Facebook has been roundly criticized for being slow to acknowledge a vast disinformation campaign run by Russian operatives on its platform” (Issac and Frenkel, 2018). It was stunning to much of the online community of users and the media that data stored by multibillion dollar corporations was not secured. Americans had been appalled with the misuse of data for the purpose of driving “fake news” into population with the underlying motive of directing outcomes in political elections. The result of these accidents negatively affect companies like Facebook; they lose public trust, online users, company growth, and they ultimately are not able to operate their once-thriving businesses. This is not the first time a cyberattack has breached a company holding a sizable user basis, “The Facebook bug is reminiscent of a much larger attack on Yahoo in which attackers compromised 3 billion accounts - enough for half of the world's entire population.” (Pioneer, 2018). Companies of this scale should aim to build trust. Many of their online users are actively involved in various online services, and these users should trust the safety of their data when using platforms like Facebook to bring more business to themselves as well as Facebook, by self promotion and advertisement.

Across industries like banking and healthcare, core services will soon be digitized. One enormous example would be online banking, “Many financial institutions have implemented, are in the process of implementing, or are planning to implement some form of Internet presence by providing services online” (Saleh, 2003). However, even with all of these capabilities, security concerns about confidential information and data arise when any form of personal information is put onto the Internet. Many of these services will require agreement of online policies as well as terms and conditions for access. These industries resemble social networking sites that provide content and services too. Many of the businesses within those industries would be advantageous to take on broad views of responsibility in addition to stronger privacy settings and robust security practices before any online misuses or breaches of data arise.

Legal Issues

At the present, there are limits legally to the power and jurisdiction that government bodies have on data security. Even in areas where data protection is strong, legislation must keep up with new developments in technology. Information technology is a field that is continually growing and around the world, data protection is struggling to stay in line with legislation. As a result, data protection is not legally applied uniformly across borders; data protection policy often depends on what country a person is in. There is a need to establish a set of guidelines or policy for online privacy and security. This need is relevant internationally, for example, countries associated with the European Union comply to the General Data Protection Regulation

(GDPR). Countries who agree with the GDPR are up to date on legislative standards of how personal data is properly handled as well as what is categorized as personal data (Judicature, 2018). They move forward discussions on data security across every industry by reshaping the ethics behind data protection.

Ethical Issues

The outcome of approving the GDPR, as well as the recent changes in data privacy, has led to set a standard of ethics in data protection. The GDPR is something likened to the known prototype of universal standards in data protection. In order for data protection to become more widely accepted and complete, a major number of developed countries would need to come to an agreement on what would be acceptable data protection laws in addition how terms such as personal data are defined. In doing so, data protection can become more unanimous and overcome slight differences in perspectives and methodology among different countries.

In another arena, the political arena, the ethics of data protection has reached a new level of political significance, “News broke early this year that a data analytics firm once employed by the Trump campaign, Cambridge Analytica, had improperly gained access to personal data from millions of user profiles” (Pioneer, 2018). The ethical concern here is not only improper access, but also the misuse of information. This event has revealed the moral gray areas of how data can be accessed or used. The group that carried out this strategy also misused data by employing “fake news” campaigns as well as advertising and driving misinformation to the public in order to steer the direction of a political outcome.

Future use

In the near future, data protection and security could potentially breed businesses that provide more satisfying on demand services as well as products. These more marketable businesses could also advertise upcoming changes that are suggested or relevant to consumers. Furthermore, in order to bring the consumer back for more business, data protection and cyber security need to be more consistent and able in order to foster trust with users and corporations alike.

Instead of easy access upon agreement, stronger security practices can be fostered by providing better developed acceptable use conditions that might educate users on what risks and threats to data can be. These conditions could even train users in appropriate behavior and safe usage of platforms online. Social networking sites like Facebook should uphold standards of data protection like the ones previously mentioned. In addition, establishing oversight on third party apps from advertisers can monitor misuse or improper gain of access to personal data. Furthermore, Facebook should employ cyber security teams to proceed in information audits of third parties who are using suspicious methods and terms of service. These are a few of the ways that social networking sites can build trust with users to improve and promote more business. Recent breaches in large social networking sites like Facebook demonstrate the importance of data protection and privacy. Furthermore, they reveal that data is not secure to a certain standard; companies are not taking on full responsibility of data breaches; and users have not realized the extent and importance of their data footprint. Resolving these issues will boost the online business activity and trust that is built into social networking sites, even after data security breaches and scandals.

Annotated Bibliography

Brownstein, R. (2013, Jun 13). Americans know they've already lost their privacy.*National Journal,* Retrieved October 1, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/1418386941?accountid=14541

- This scholarly journal references the clear upsides to using online services. In addition, it highlights how Americans feel about the positives and negatives of being on the Internet to access different services and products that they want to use. Upon consent and access to social media platforms, benefits referenced within the paper relate to : communicating and connecting, better access to information as well as sharing it, and finally safety of the public. This material is accessed as very reliable; it uses statistical data, includes anecdotes, and even create more understandable and relatable measures of privacy index among different respondent age groups. This scholarly journal details interviews of groups of people on the idea of privacy erosion due to the Internet and increasing oversight and surveillance from the government.

Bull, M. (2013, January 13). *Effects of Social Media on Internet Privacy*. Retrieved October 1, 2018,

from https://www.michael-bull.com/articles/ethics-essay.pdf

- This source is a well rounded literature exploring the relationship of social media and Internet privacy. Written only five years ago, the author details the subject of data privacy that is provided by social networking platforms. This source is deemed reliable because of how the author presents his thoughts. Along the paper, in text citations of definitions are often used to present a clear idea of the information. Details that are referenced in the paper relate to the responsibility of users, but more so developers who can add sufficient privacy control tools to their sites. In addition, the details of educating users is referenced in the paper to support the idea that privacy can start with correctly informing the user of what can threaten privacy and what activity can carry risk to the online user.

Decoding GDPR. (2018, May). *Judicature, 102*(1), 58-66. Retrieved October 1, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2098960409?accountid=14541

- This is a well known scholarly journal and magazine written to explain judicial systems in layman's terms. This source is known to be reliable and has been around since 1966. The details of the journal reference the General Data Protection Regulations recently passed in the European Union. The journal “decodes” and presents the new regulations for data privacy in understandable pieces. In addition, the journal explains the core reasoning to the GDPR and how it affects online users and their privacy within the European Union. The journal is referenced for the background behind the GDPR and the definitions that the EU would like to make clear to the public as well as the online community.

Issac, M., & Frenkel, S. (2018, September 28). Facebook Security Breach Exposes Accounts of 50 Million Users. Retrieved October 1, 2018, from NYTIMES.com website:

https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html

- This is a well known print and online magazine with well known writers; this article and its details are referenced in the paper. The New York Times is definitely a reliable source with millions of paid subscribers nationwide. The reference used relates to the “fake news” campaign run by foreign agents from Russia to affect outcomes of the most recent presidential election. This online magazine also highlights actions taken by Cambridge Analytica in Trump’s campaign. The NYTIMES state that personal information of millions was collected from Facebook improperly by Cambridge Analytica. The magazine also details how difficult it can be to secure the whole system that has billions of users and is connected with countless third-parties.

Matsakis, L., & Lapowsky, I. (2018, September 28). Everything We Know About Facebook's Massive Security Breach. Retrieved October 1, 2018, from WIRED.COM website: https://www.wired.com/story/facebook-security-breach-50-million-accounts/

- This is a website reference that is known to many in the online community. Wired.com is a reliable website that provides up to date news on all things in the business of electronics, technology, and science! WIRED.com has a large following is deemed a reliable source without much scandal, accidents, or error of their company in recent years. The writer in this article explores the recent privacy issues that are happening with Facebook. They recent data breach that exposed 50 million users is covered as well as the prior Cambridge Analytica scandal affecting Facebook. The reference in the paper covers the details of how the issues in data security resemble an “arms race”. This arms race described is one that relates to the efforts of technology giants to consolidate data privacy and security so that problems and accidents do not arise in the first place.

Saleh, Z. I. (2003). *An examination of the internet security and its impact on trust and adoption of online banking* (Order No. 3119851). Available from ProQuest Central; ProQuest Dissertations & Theses Global. (305213244). Retrieved October 1, 2018 https://search.proquest.com/docview/305213244?accountid=14541

- This source is a scholarly paper taken from ProQuest. The paper is a graduate dissertation on the relationship between internet security and online banking. The details of the dissertation are referenced in the paper to explain how and why services on the Internet are used. In addition, the paper references how banks and other large institutions are using the Internet to carry out transactions. These changes are not without important security concerns and risk involved with the progress of the new innovation and accessibility of online banking. This material is reliable; the source uses in text citations of well known sources. It should also be noted that the paper is a dissertation thesis for the degree of Doctor of Philosophy, so it must have been review a countless number of times by high achieving academics.

What's next after FB's data breach? (2018, Oct 01). *The Pioneer* Retrieved October 1, 2018 from https://search.proquest.com/docview/2114406 364?accountid=14541

- This scholarly article is written by an airline magazine in India that reviewed the most recent data security breach to affect the company Facebook. On September 25, 2018, Facebook was the subject of a cyber attack that allows access to 50 million accounts. The magazine informs the public that the attack is anonymous and that it did not break the trust of the 2 billion global users yet. The material is assessed as reliable and is referenced twice within the paper to highlight other cyber attacks that have affected other large technology companies such as Yahoo. This material resource is published by a popular airline; it is a magazine for international travelers to receive urgent updates on several industries and their important news.