Memorandum on Privacy and Data Protection

Michael Greene

Old Dominion University

CYSE 406

October 21, 2022

To: Governor Tar-Miriel

From: Michael Greene

Subject: Privacy and Data Protection

Date: October 21, 2022

This memo is to inform you Governor Tar-Miriel on the importance of privacy in this modern age. With increasing advances in technology, society has grown to accept and depend on this technology. Accompanying this change in society has been our perception of privacy. As we know privacy is an individual's way to express themselves in an environment, they feel is secure preferably from public view. Most people in society now associate privacy with the digital medium. With the advent of the internet connecting people across the world, society has begun conducting business, storing personal data, and spending their leisure time on the internet. This data at times contains personal information and data on an individual, that revealed to the public can cause serious problems to that individual and the reputation of the organization entrusted with said information. Not only is this data appealing to malicious actors, but also to the companies entrusted with this information. These organizations see the value in this information and have at times been caught selling this information for marketing and research purposes without the individuals consent or even knowledge. For instance, Facebook in 2018 was discovered to have collected and provided data to Cambridge Analytica without user's consent (Ma, 2019). Without regulations or a means of holding organizations accountable, organizations such as Facebook are capable of eroding what little privacy we may have unopposed. The result could lead to a loss of public trust between society, governments, and big corporations. It could also lead to personal and financial damage to the individual such as identity theft.

The information that society seeks to protect when it comes to privacy concerns is referred to as Personally Identifiable Information or PII for short, and Biometric data. The Department of Homeland Security defines PII as any information or collection of information that can either directly or indirectly be linked to an individual (*What is personally identifiable information?*). For example, knowing only a first name may not be enough to identify a particular person, but in combination with a last name and race. The information may lead to the identification of a particular person. Again, using the DHS definition, Biometric data on the other hand is identified as the physical characteristics unique to an individual that could be used as a means of verification to gain access (*Biometrics*). An example of biometric data would be a fingerprint sensor on a phone. The phone stores a copy of your fingerprint and references this data to unlock your phone. The common trait between theses two is the fact that all this information is unique to an individual. In simpler terms, biometric data refers to physical characteristics of an individual as PII refers to descriptive data of an individual. This information is important to an individual, with governments around the world realizing the need to protect this data.

The European Union has recognized the importance of regulating this information and has set an example for other countries to follow with the implementation of the General Data Protection Regulation. The GDPR provides a means of holding organizations accountable for

users' information simultaneously giving greater control over the data shared by users. Organizations handling users' data must be transparent with users on what data will collected, how it will be handled, request consent from users, and provide the ability for users to remove data that was provided to name a few (Burgess, 2020). If a company is found in violating a user's privacy, the GDPR can hold that company liable. There are exceptions to the GDPR in the event that national security is at risk, or the possibility there is an ongoing investigation into illegal activity. The GDPR also only applies to those primarily conducting business online, so private matters are not covered under the GDPR. Another important note to point out regarding the GDPR is that European citizens and residents are covered under the protection of the GDPR. So, any organization wanting to conduct business with EU citizens must comply, despite the fact they may be located outside the EU. This law has been a major step for how to implement regulatory measures on electronic media, so much so that some states in the United States have adopted a similar approach for protecting consumers.

California for example introduced the CCPA or California Consumer Privacy Act. This act was modeled after the GDPR and retains many similar attributes from the GDPR. For example, organizations handling California residents' data must be transparent with what is collected, knowledge of where this information has been disclosed, options for removal, and requesting consent (*California Consumer Privacy Act (CCPA)* 2022). However, some key differences between the CCPA and GDPR should be mentioned. For instance, information already publicly available provided by the federal and state, financial reports related to credit reporting, and smaller organizations that handle less than 50,000 California residents. While the CCPA may not be as stringent or encompassing as the GDPR, it still remains a good starting point for others to follow and hopefully influence the Federal government into regulating user data.

This is why Governor Tar-Miriel I believe that pressure on having a regulatory standard on handling user data should be a priority within the Federal Government. Other nations and even the state of California as mentioned before, have recognized the importance of protecting consumer data and have taken the initiative to implement their own laws to protect users. Technology will only continue to advance rapidly at a pace policy makers may not be capable of keeping up with. Without a means of regulating organizations that handle user data, they will continue to exploit users for profit. By providing a means of holding organizations accountable for the data they are entrusted with. These organizations would take more consideration in handling user data for fear of repercussions. This would also provide some amount of trust with the general public, knowing that their information is safe and proper procedures are in place should an incident occur. Not having a set standard would also allow for organizations to implement their own interpretation of how to handle privacy. So, one organization may have lax handling policies due to there no standard to be followed. However, with change also raises both foreseeable and unforeseeable issues. Such as the risk of having big corporations leaving the country to move to areas with relaxed regulations. This may have a negative effect on the economy with jobs at risk. Initial implementation may lead to confusion and constant revisions in order to satisfy all parties. There may also be extra costs for organizations having to restructure current policies and security measures for user data in order to be withing standards. Despite all these risks Governor Tar Miriel, I personally believe users data needs regulating and protection. The data they provide is theirs, and they should have a right within reason to control

that data. Exemptions can be made for harmful or illegal activity, but other then that no one should be profiting off of other people's information.

References

Biometrics. Biometrics | Homeland Security. (n.d.). Retrieved October 20, 2022, from https://www.dhs.gov/biometrics.

Burgess, M. (2020, March 24). *What is GDPR? the summary guide to GDPR compliance in the UK*. WIRED UK. Retrieved October 21, 2022, from https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018.

California Consumer Privacy Act (CCPA). State of California - Department of Justice - Office of the Attorney General. (2022, March 28). Retrieved October 21, 2022, from https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20requires%20business%20privacy,the%20Right%20to%20Non%2DDiscrimination.

Ma, A. (2019, August 23). *Facebook understood how dangerous the trump-linked data firm Cambridge Analytica could be much earlier than it previously said. here's everything that's happened up until now.* Business Insider. Retrieved October 21, 2022, from https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3.

What is personally identifiable information? What is Personally Identifiable Information? Homeland Security. (n.d.). Retrieved October 21, 2022, from https://www.dhs.gov/privacy-training/what-personally-identifiable-information.