REFLECTION ESSAY

Privacy and Security

Jiebin Zhu (Alex)
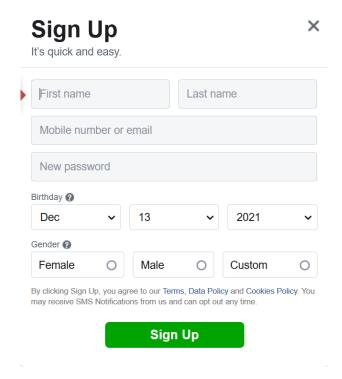IST 618 Fall 2021

INTRODUCTION

In the United States, people are aware that the government surveillance programs are common nowadays. The topic on government surveillance that was leaked by a whistleblower, Edward Snowden, in 2013, had truly changed many discussions of national security when individual privacy comes into the spotlight. For examples that will be used to put things into better context throughout this essay in the national security and individual privacy scope, the US government would be mentioned regarding the data it collects from its citizens. In addition, an example for a company that is based in the US and collects data from its customers, Facebook, would also be mentioned later as a comparison for government versus private business. In the comparisons, advantages and disadvantages would be listed out for both government and Facebook regarding the way they utilize personal information. Furthermore, I will also choose a side that I would be the most concerned about when information privacy comes into play and mention some potential ethical dilemmas that these two sides have when collecting personal data off its citizens/users. Lastly, I would try to recommend some ways of protecting privacy with potential policies that can be implemented along with its pros and cons.

GOVERNMENT'S COLLECTION OF DATA

Based on what Edward Snowden had mentioned regarding the highly classified information he shared with the public, the US government is able to collect whatever they want with using intercepts (MacAskill, 2013). His sharing of this information was very important to the passing of the USA Freedom Act in 2015 and allowed the government to create some limits on any bulk communication of telecommunication data. In a country where telecommunication is probably the main source of communication, this pretty much stopped the government from collecting data whenever they wanted like how they did it before. Other than this type of data that the government can collect which is associated to our activities in the digital world (like a digital footprint), they already have information on who people are as individuals. They have access to our names, addresses, social security card information, phone numbers, credit history, etc.

FACEBOOK'S COLLECTION OF DATA

Facebook is a platform and app that users interact with to connect, document, and share their life events or status with their social network. The image below is obtained from Facebook.com when trying to simply create a new account. It shows the very minimal information Facebook needs for a user to even have access into their service such as name, phone or email, password, birthday, and gender.

This is just very basic information that Facebook collects because if a user is willing to fully experience this platform they can provide data about their education, city they live in, languages they speak, etc. in their profile which is stored in Facebook's databases. Essentially, data that personalizes an individual is the data that Facebook is trying to collect here.

ADVANTAGES OF COLLECTING AND USING PERSONAL DATA

For US governments, the main purpose of them collecting and using personalized data is for security measures. They use a significant amount of data to build out profiles to help detect and prevent any type of security breaches, fraudulent activities, terrorism, etc. (Dinev et al., 2008). In addition, this a lot has changed after 9/11 so this justifies the collection of data and usage of it.

For Facebook, its sole purpose is for monetization. It allows users to connect with each other due to the network externalities structure of a social media company. Having a large user base due to that allows the company's business model to run advertisements for revenue and target certain users. Like the US government, they use their users' data to build profiles for them and understand their consumer preferences (Dinev et al., 2008). Understanding their user's taste allows them to target them with

specific advertisements using the algorithm that's generated based off that profile. It personalizes the choice for the user and potentially offer them what they want.

DISADVANTAGES OF COLLECTING AND USING PERSONAL DATA

When some entity, whether it's a government or private business, collects personal information from people they are keeping and using the most sensitive data those people have. Since privacy is among the highest individual rights (Dinev et al., 2008), this would cause distrust in government such as what happened after Snowden went public with his information. A great example for distrust in the government would be the COVID-19 contact tracing failure, because of the distrust people had in government obtaining their data (Lewis, 2020). Even way before the Snowden incident, people were already afraid of their erosion of privacy in the past already (Dinev et al., 2008). In a more recent case of Facebook here, there was a breach in their system that had leaked their users' data online (Holmes, 2021). Collecting all that data, brings the risk of potential breaches that could leak all that out. There are just so many cases of these types of activities happening on recent events like the SolarWinds breach or Twitch.tv breach.

MOST CONCERNED SECTOR IN RELATION TO INFO PRIVACY

For me personally, I would be a lot more concerned about the fact that a lot of private businesses like Facebook have my information even though they only use it to display products or services I might want to purchase. That is an amazing win-win situation, but at the end it is only about advertisements, and benefiting my desires. It's been seemingly common to me how private businesses have been getting breached, so I would be really concern if my information stayed within their systems. Data breaches has been becoming more recent, a recent example of Log4j vulnerability has been discovered and it's creating concerns everywhere (Newman, 2021). People are trusting companies with their own sensitive information, but when a breach occurs, and the data gets compromised that would significantly lower the trusts in these companies. I wouldn't mind providing information to the government or their surveillance program if it could assist them with the national security efforts they are doing. With that in mind, I shall remain hopeful that our data would be safe in their hands and their cybersecurity team to protect it.

POTENTIAL ETHICAL DILEMMA

The most prominent ethical concern here when dealing with personal information is the potential violation into personal privacy. From the government's side, they have some ethical dilemma here

regarding collecting personal information for sake of national security (Garcia-Murillo). This was pointed out earlier in Snowden's big reveal of government surveillances on the people. In addition, this issue was a huge concern for librarians who work hard to protect their patron's data and had to "fight" with the government to get policies adjusted (Garcia-Murillo) because government before were able to collect data in bulk for security purposes, but that contradicts one of the librarians' responsibilities. On the other end here, relates to how Facebook could be facing some ethical dilemma. In their business model where they rely on target advertisements and providing data to 3rd parties, they've been put on the spotlight a lot recently in relates to how they are using the data that they've obtained from users such as the Cambridge Analytica incident that had probably had some influences in the 2016 presidential campaigns. Another example here would be rather recent in how a former Facebook employee revealed that the company would prioritize profits over safety and role that the company plays for the insurrection on Capitol Hill and the contents that children may see on the site (Diaz, 2021).

POLICY RECOMMENDATION

It's hard exceptionally for the government to create policies that is one size fit all in this country regarding the collection of personal private data. I believe that a lot of politicians that sit in Congress and the Senate don't understand how ICTs work fully these days from their questions and responses in understanding how Facebook works. This means that support is needed from many of the leading ICT companies to cooperate on a policy that helps protect privacy but doesn't affect the national security. I personally side with the realm of national security a bit more here so my recommendation might be a bit biased.

My recommendation is for the government to still be able to collect personal information on communication devices and platforms when needed with full transparency, and ICT companies would need to provide aggregated data to the government if need be and the government can ask for an individual's data with a court order only. Regarding full transparency, this should let the individual be notified via their contact method after a certain time if their very sensitive personal information was accessed by the government what type of information and what specific information was accessed. The time should be implemented depending on if letting the individual know would jeopardize the investigation. The benefits of this are to still allow the government to run their data models with aggregated data sets for security purposes if needed while protecting most individual's data and also

provide visibility into what was accessed specifically since that information can be directly traced to an individual. The drawbacks, however, is that this policy might receive low support since it still allows the government to access a person's data. It would also be hard for ICT to implement by providing aggregated datasets since the volume of data is too large nowadays and there's a lot of unstructured data on the web that makes it expensive to clean and prepare. In addition, the companies would also need fundings from the government to implement it.

CONCLUSION

Overall, the collection of data that's being done whether in the context of government or by private companies like Facebook would get into the realm of intruding personal privacy. Governments have the concern of the national security in mind and Facebook is only doing it to its users for monetization. These two different types of entities also have a major concern in mind and that's cybersecurity and that would be a group effort to keep adversaries away from accessing personal data. Lastly, to implement new policies to collect personal information the government and ICT companies would need to work together.

Word Count: 1661

Work Cited

Diaz, J. (2021, October 4). *Facebook's new whistleblower is renewing scrutiny of the social media giant*. NPR. Retrieved December 19, 2021, from https://www.npr.org/2021/10/04/1042921981/facebook-whistleblower-renewing-scrutiny-of-social-media-giant

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance – an empirical investigation. *The Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Garcia-Murillo, M. IST 618-Information Policy, Ethics lecture

Garcia-Murillo, M. IST 618-Information Policy, Security lecture

Holmes, A. (2021, April 3). *533 million facebook users' phone numbers and personal data have been leaked online*. Business Insider. Retrieved December 13, 2021, from https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

Lewis, D. (2020, December 17). *Why many countries failed at COVID contact-tracing - but some got it right*. Nature News. Retrieved December 13, 2021, from https://www.nature.com/articles/d41586-020-03518-4.

MacAskill, E. (2013, June 10). *Edward Snowden, NSA files source: 'if they want to get you, in time they will'*. The Guardian. Retrieved December 13, 2021, from https://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why.

Newman, L. H. (2021, December 10). *'the internet is on fire'*. Wired. Retrieved December 13, 2021, from https://www.wired.com/story/log4j-flaw-hacking-internet/.