Adrian N
an9905
Cyber Security Policy & Law
Midterm Paper – The Data Economy

Introduction:

A growing number of online entities are collecting vast amounts of personal data. Data mining and advances in data analytics now make it possible to infer sensitive information from data. This relatively new commodity spawned a fast-growing industry which is prompting antitrust regulators to step in to restrain those who control its flow. A century ago, this resource was oil, but thanks to giants like Alphabet, Amazon, Apple, Facebook, and Microsoft the new commodity is data, the oil of the digital era. The biggest problem facing this data collection comes from antitrust. Antitrust laws are statutes developed by governments to protect consumers from predatory business practices and ensure fair competition. This antitrust is the reason it should be mandatory that the user have complete control over their data. To proactively solve this problem, the US should pass a federal data control law that offers more user control over data collection.

Audience:

The FTC, or the Federal Trade Commission, could make the changes necessary to advance the cyber security in the data collection world as they have the power to do so. They should also be obliged to be motivated as the agency is responsible for enforcing the prohibition on “unfair and deceptive acts or practices”. This is somewhat vague, so unfair data collection does fall into this category. It is also evident that even when big companies support a data collection law regarding privacy, the goal of their ‘involvement’ is to weaken and dilute consumer protections. We cannot solve the privacy “crisis” by treating information as the

personal property of those to whom it refers or by adapting the systems for protecting copyright, patent, and other so-called “intellectual property” to personal information (Downes 1). Assuming a law would be passed this would be a huge ask, and a complicated one, so we must make sure it is effective and ticks off as many bullet points as possible. Big tech companies like Facebook, that are currently collecting huge amounts of data have a lot of control in this sector and need to show their userbase that they care about their privacy by recommending and approving good legislation.

Problem Statement:

From toilet seats to refrigerators—all sorts of devices are becoming sources of data. The reason this is important is because we are all victims when it comes to the online world. We are all victims of spam, adware and other unwelcome methods that try to get our money. Most online targeted marketing is far better than blanket marketing and can sometimes be very useful. However, to achieve this, advertising organizations need to track and hold a significant amount of information about users and their preferences. Some of this can be personal, such as age and location. When companies are tracking spending profiles and the types of products people buy, this data can become very sensitive. The marketeers are gathering huge amounts of information and then mining this for marketing purposes. This data can also be misused for nefarious purposes if it gets into the wrong hands. One example of this is unauthorized use, like what happened recently in 2016. Following the 2016 United States presidential election, the news came out that Cambridge Analytica had obtained the data of millions of Facebook users which was used in campaign advertising (NY Times 1). This is obviously huge as there are powerful stakeholders involved now, making this a national cyber security problem. Another

problem that arises from this is the concept of a monopoly of data collection. Big companies will get too much of the data and control what goes where. An example of where this can go bad is if a company collects important health data for example of cancer patients. They easily could charge any researcher a premium for the data making gaining access to important information that may lead to life saving developments out of reach for some firms / organizations. In all, the data economy must be dealt with as our data must be protected and used for the right reasons, and it cannot be evaded.

Primary Tension:

When it comes to data collection in the modern era, there are two main things companies focus on when it comes to managing data collection. This is the tension between the balance of innovation and security/privacy. Knowing this, data collection is useful as it allows for a wide variety of data that could potentially lead to better and faster innovations. Going back to the example of health information, health technology has created a huge market for data collection. Potential feedback on patients and doctors will lead to more information that developers can use to create more personalized and powerful technology. On the flip side of this, there is a huge decrease in privacy from the user. Today, when data is collected by the agencies and businesses, the individual people supplying the data no longer have control over their personal information. This lack of privacy may be concerning to people and most of the time they cannot do anything about it if they want to continue using the service provided. Along with this is security as storing tons of data, including extremely personal information like bank account information and health records, require strict security. As we have learned,

hackers are always hard at work looking for ways to bypass these controls to gain access to data.

Mark Zuckerberg promises that Facebook can do better to protect our privacy. Three times during his testimony before Congress on Tuesday, he used the same example: Face recognition technology, he explained, should require "special consent" from users. He left out a key face: This week, lobbyists paid by Facebook are working with Illinois lawmakers backed by Facebook to gut the state's face recognition privacy law, the strongest in the nation… We cannot underestimate the tech sector's power in Congress and in state legislatures. If the United States tries to pass broad rules for personal data, that effort may well be co-opted by Silicon Valley, and we'll miss our best shot at meaningful privacy protections (Alvaro 1). Clearly, everything starts with Silicon Valley, and I believe that a company like Facebook could pave the way for other tech giants to follow and set a precedent that will be remembered forever. If this law were to get passed, Facebook can stop spending capital on these Lobbyists and focus on creating different analytical software to better personalize ads. In the end I believe there might be even more data to collect if people were paid to give it up, especially if a big company like Facebook were to gain this trust with their userbase. Data collection could continue if there was more user involvement and knowledge.

Recommendation and Rationale:

A work around for this is to allow the user to have more control over their data. There is a ton of ways you could go about this as seen in the Economist article. In the text it states, "Oracle, which dominates the market for corporate databases, for example, is developing what amounts to an exchange for data assets. It wants its customers to trade data, combine them

with sets provided by Oracle and extract insights--all in the safe environment of the firm's computing cloud, where it can make sure, among other things, that information is not misused... Citizenme allows users to pull all their online information together in one place and earn a small fee if they share it with brands. Datacoup, another startup, is selling insights from personal data and passing on part of the proceeds to its users (The Economist, 2017).” These smaller companies in comparison to the titans are proceeding in the right direction. Most of the time many services we use daily make us sign a terms & conditions contract that are often impenetrable and leave the user with no choice other than to accept them. This is appalling and forces the user to make decisions they may not agree with. A solution to this is to offer a contractual agreement of sorts in which the user is in control of their data. There could be an option in which the user opts to give his or her information for free if they believe in the greater good their data could do. For example, a medical situation where the user does not want to profit if they know their information will be used to save another humans life. However, when it comes to social media applications for instance, it would be beneficial if the user controls where their data goes and how it is used and maybe have the user make money in exchange for offering up their information. This recommendation is not the only recommendation however as seen in the same article. It states, “In 1911 America's Supreme Court upheld a lower-court ruling to break up Standard Oil, which then controlled around 90% of oil refining in the country. Some are already calling for a similar break-up of the likes of Google, including Jonathan Taplin of the University of Southern California in his new book "Move Fast and Break Things" (The Economist, 2017).” This excerpt is what some people believe to be the solution to this new antitrust problem of data collection. However, this cannot be the solution because this would

not really solve the problem, as a breakup would slow down innovation exponentially, also leading way for a Googlet or a Babyface to become dominant again. Therefore, the original solution of a more user-controlled data collection method would be the most beneficial. If we were to allow the user to fully have control over their data, I believe that these users will still offer up the information if they know it is for the greater good, or in some cases if they get paid. Digital data is not referred to as modern day oil in terms of a commodity for no reason, and there is enough money to go around.

References

Bedoya, Alvaro M. “Opinion | Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills.” *The New York Times*, 11 Apr. 2018, www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html. Accessed 10 Dec. 2021.

Confessore, Nicholas. “Cambridge Analytica and Facebook: The Scandal and the Fallout so Far.” *The New York Times*, 4 Apr. 2018, www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Fuel of the future; the data economy. (2017, May 06). *The Economist, 423*, 17. https://ezproxy.rit.edu/login?url=https://www.proquest.com/magazines/fuel-future-data-economy/docview/1895923853/se-2?accountid=108

Midterm Paper – Facial Recognition

Introduction

Facial recognition is a way of recognizing a human face through technology. From unlocking our mobile devices to tagging our friends in Facebook posts, this type of biometric technology makes authentication quick, simple, and (most of the time) accurate. However, facial recognition has also been the subject of plenty of controversies, especially in the aftermath of the shooting of George Floyd, which drew attention to the racially motivated police brutality in the US. Due to many police forces relying on facial recognition technology to identify potential suspects, tech giants such as Amazon, Microsoft, and IBM had chosen to reconsider their stances on its development and sales. Weeks later, the use of facial recognition for law enforcement purposes was also deemed unlawful in the UK, with the Court of Appeal declaring that the technology violates human rights, data protection laws, and equality laws. To combat this facial recognition technology problem, the US should pass a federal country wide law that bans the use of facial recognition software by the police and all other municipal agencies.

Audience

San Francisco has taken a stand against potential abuse by banning the use of facial recognition software by the police and other agencies. This made San Francisco the first major American city to block a tool that many police forces are turning to in the search for both small-time criminal suspects and perpetrators of mass carnage (Conger 2019). A federal privacy law will be monumental, so it is necessary that every party compromise and agrees on the diction in the law. The government must show us that they respect our first amendment rights, along

with our personal freedom and societal privacy. Seeing as San Francisco being the real and perceived headquarters for all things tech advocate for the regulation of facial technology means a lot as they are taking initiative and setting precedents for cities, states, or even country wide legislation to be passed.

Problem

Organizations of all sectors are adopting facial recognition fast. Thus, there is a lingering risk of not planning for all unintended consequences. There are big worries that face recognition technology allows governments to undermine privacy rights. Recently it was seen in action as the authorities used the technology to help identify the suspect in the mass shooting at an Annapolis, Md., newspaper last June (Conger 2019). Although, it seems a legitimate use, the line that separates that from what could constitute violation of privacy is fragile. It is even possible that some rogue elements inside government agencies misuse facial recognition to get information, and possibly using it to pursue their own private agendas or even to sell it to interested parties. Another big problem is how out of date current legislation is, as described by Mr. Abrams, "Here we have 21st-century judges addressing 21st-century technology to see if they're consistent with an 18th-century document" (NYTimes 2020). New legislation will be inevitable, and these fraudulent practices will cease.

Tension

There are two competing priorities for the government when it comes to managing the balance between privacy and security. The current trend of developing facial technology has the potential to strengthen security measures by giving the government enough access to pick out a potential perpetrator who is wanted. However, this requires access to so much data,

specifically billions of photos, that threatens an individual's privacy. Being recorded and scanned by facial recognition technology can make people feel like they're always being watched and judged for their behavior. On top of this, police can use facial recognition to run everyone in their database through a virtual criminal lineup, which is like treating one as a criminal suspect without probable cause.

An example of this in the modern day is seen in the Clearview AI case. "Clearview AI has scraped billions of photos from the internet, including from platforms like LinkedIn and Instagram, and sells access to the resulting database to law enforcement agencies. When an officer uploads a photo or a video image containing a person's face, the app tries to match the likeness and provides other photos of that person that can be found online" (Kashmir, 2020). Companies like Clearview AI will continue to do so until they are legally not able to, which knowing the court system may be a while. That is why it is best the government takes charge in the fight for our rights as the current legislation is not up to par.

Ultimately, face recognition data gets stored in servers, usually accessible via the cloud. As with any other computer system, it is vulnerable to hackers. With data breaches, face recognition information could fall into the wrong hands. Although systems are getting better at preventing identity theft, it could still happen, especially with the amount of attention it would get. Facial recognition technology is not all about its cons, as it also presents many advantages. All we need is for government action to regulate and make sure that businesses developing facial recognition technology identify and mitigate these risks, by clearly defining the boundaries for their projects, and to develop privacy policies and manage communications with their customers.

Recommendation

To rationalize the growing problem of face recognition, the United States must pass a comprehensive and strong federal law. This law could look like an updated version of our first amendment, just more applicable to modern day by mentioning current computer capabilities. On top of this, it should be just vague enough to be flexible and adaptable to combat the constantly changing cyber world. This law should also take inspiration after the state of Maine and their laws in which regulate government use of facial recognition. Maine's new law prohibits the use of facial recognition technology in most areas of government, including in public schools and for surveillance purposes. It creates carefully carved out exceptions for law enforcement to use facial recognition, creating standards for its use and avoiding the potential for abuse we've seen in other parts of the country. Importantly, it prohibits the use of facial recognition technology to conduct surveillance of people as they go about their business in Maine, attending political meetings and protests, visiting friends and family, and seeking out healthcare (ACLU 1). Ideally, a US law would not prove to be to out of line for the police to disagree with, as it still gives them some flexibility to use the facial recognition but cannot be the main source of evidence in a trial and cannot be used without probably cause.

To companies that are currently collecting, processing, and selling large amounts of data, such a law may seem harsh and unappealing, but after the initial adjustment period to the new law, it would improve business efficiency and lay a better framework for what to follow. This would help avoid potential lawsuits that they would face currently, and in general save them money in that aspect. It would also prove to be great for the government and police as well as although the technology is not at 100 percent, and probably never will

be perfectly accurate, it can at least be successful in at least providing some leads to criminal investigators. As competition brews in the market facial recognition will get stronger and stronger and will prove its worth, if it is regulated properly and protected safely, it should not pose a problem to the public.

This law will bring the same benefits all parties wanted and at the same time, it will prevent the compliance disaster that would result from 50 state-level privacy laws with varying requirements regarding facial recognition. By mirroring the Maine existing legislate, companies who already do business internationally with places like the UK or in San Francisco will not see much of a change, and those that wish to expand to other places will be able to do so easily. This law will provide a framework that is easy to comprehend and follow because it is written in modern day. The government will also gain trust with the public again as their use of facial recognition will be forced to be more open. Facial Recognition companies and police bodies should advocate for a federal law rather than fearing and fighting against one because it has too many potential benefits to all people.

References

"ACLU News & Commentary." *American Civil Liberties Union*, www.aclu.org/news/privacy-technology/maines-facial-recognition-law-shows-bipartisan-support-for-protecting-privacy/. Accessed 12 Dec. 2021.

Conger, Kate, et al. "San Francisco Bans Facial Recognition Technology." *The New York Times*, 14 May 2019, www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

Hill, Kashmir. "Facial Recognition Start-up Mounts a First Amendment Defense." *The New York Times*, 11 Aug. 2020, www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html#:~:text=Clearview%20AI%20has%20hired%20Floyd. Accessed 12 Dec. 2021.