

### **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 marketers 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. 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. Cognitive Logic, a startup, has come up with a similar product, but leaves the data in separate IT systems. Other young firms hope to give consumers more of a stake in their data. 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](http://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](http://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>