DATA PRIVACY STANDARDS IN THE UNITED STATES: A CASE STUDY OF FACEBOOK

Presented by Michael Pearce Blend

in partial fulfillment of the requirements for completion of the
Evidence and Inquiry certificate and the
Polymathic Scholars honors program in the College of Natural Sciences at
The University of Texas at Austin

Spring 2020

Supervised by:

Angela C. Beasley, MSCS
Department of Computer Science
The University of Texas at Austin

Second Reader:

Rebecca A. Wilcox, Ph.D.
CNS Honors
The University of Texas at Austin

I intend to submit a copy of my Polymathic Scholars thesis to the Texas ScholarWorks (TSW) Repository. For more information on the TSW, please visit https://repositories.lib.utexas.edu/.

Data Privacy Standards in the United States: A Case Study of Facebook

_____ _____

Michael Pearce Blend Date

Table of Contents

Acknowledgements

I would like to thank Professor Angela Beasley in the Computer Science Department at the University of Texas at Austin for all her help in my thesis writing process. She spent much time reviewing and critiquing my writing and providing suggestions for expanding upon my original topics. I am grateful for working with such a helpful and flexible supervisor.

Next, I appreciate my friends and family members for their encouragement during my ambitious writing process and for reviewing drafts.

Finally, I would like to thank Dr. Rebecca Wilcox at the Honors Center in the College of Natural Sciences at the University of Texas at Austin. Her structured classes significantly helped me in undertaking such a daunting task as writing an undergraduate thesis. She gave me continued guidance and inspiration. In addition to Dr. Wilcox, I thank the entire Natural Sciences Honors Center for their efforts and support.

Abstract

With approximately 2.45 billion monthly active users as of early 2019, Facebook is the largest social media platform in the world. Facebook collects roughly one million data points of sensitive information every minute and utilizes this personal data for targeted advertisements. The majority of American users are unaware, or simply unconcerned, about the infringement of their privacy rights. Furthermore, the United States federal government has no comprehensive legislation protecting citizens' data privacy, and only twenty-five states have enforceable laws. This thesis first discusses the potential dangers of Facebook's collection of its users' personal data, including data breaches. Then, it analyzes data privacy standards in the United States and compares those standards to privacy legislation in other countries in order to make a well-informed suggestion about how our nation might protect personal data. In doing so, this thesis aims to explore fair policy solutions for the United States that keep both consumers and businesses in mind. Although the imposition of legal restraints for Facebook and others is necessary to protect individual data privacy, industry indicators reveal that placing burdensome limits on data collection capabilities could have significant repercussions for companies that provide free social media platforms, which could potentially force them to become paid services. While American policymakers must formulate and update legal measures to address data protection rights in an ever-growing data-driven economy, it is critical that reforms do not overly penalize social networking services.

Key Terms: Facebook, data, privacy rights, targeted advertisements, legal policy

Introduction

Ever since the industrial revolution of the 18th and 19th centuries, technological advances in modern society have rapidly changed the way most people around the world live their day-to-day lives. In more recent years, especially since the beginning of the 21st century, the technology industry has grown exponentially in a short period of time. With the help of Internet connectivity, the click of a button is the only act that separates us from contacting someone across the globe. Instantaneous communication technologies have initiated a worldwide revolution that has significantly transformed global economics and politics. Social media platforms are the heart of this paradigm shift. Checking Twitter, Facebook, and Instagram has become a daily habit, especially among younger generations. One of the most impactful technological improvements that has changed the way the world works in recent years is big data. The ability to collect and store extraordinary amounts of data at little cost is revolutionizing the way many businesses—not just technology companies—operate and generate income. Social media companies in particular thrive off the vast amount of personal data they collect from their billions of active users.

Any ordinary business can benefit from the optimization that data analytics provides. For example, grocery stores keep track of every single transaction and what each individual customer buys. They know that you purchased bread yesterday, and they also know that you bought eggs and coffee grounds a month ago. By keeping track of who buys what items and which products are most commonly purchased together, grocery stores create models that can predict correlations between those products. Using this information, they can strategically place items in their stores to potentially increase sales. To illustrate, if a store's predictive model identifies that

bread and potato chips are frequently purchased together, the grocery store might place potato chips and bread close together—either on the same aisle or the next aisle over—to entice customers who only buy bread to buy a bag of potato chips or customers who only buy potato chips to buy a loaf of bread.

Data analysis guides grocery store managers to place essential commodities like milk, eggs, and meats in the back of the store. The store's predictive model identifies the highest selling food items, and management capitalizes on this information with their product placement as far away from the entrance as possible. Business professors Yanliu Huang, Sam Hui, J. Jeffrey Inman, and Jacob Suher (2013) from the United States discussed this relationship between travel distance in stores to spontaneous purchases. They show how this simple, yet brilliant tactic forces customers to walk through sections of the store with less commonly sold items. Perhaps a customer will see there is a sale on the candy aisle on his or her way to pick up a carton of milk. That person most likely was only at the store to grab the basic staples for the week but now might also buy a discounted chocolate bar. This strategic store layout is just one example of dozens of ways that a grocery store uses big data and predictive modeling to boost profitability.

While the power that predictive modeling can add to the success of a grocery store is tremendous, the economic influence of this statistical technique is conceivably most prominent in the advertising industry. According to the website *Business Insider* (de Luce, 2019), "collectively, the top 200 advertisers in the US spent a record $163 billion on advertising in 2018." The site also mentions that Facebook spent $475 million on ads in 2018. Considering the prevalence of advertisements on the Internet and television, it is surprising that most Americans do not realize ads intentionally discriminate toward a certain audience. In fact, all advertisements are targeted to specific demographics, depending on the type of product or service being

promoted. For example, a cartoon channel for children on television will mainly run commercials for toys, while a news channel for adults might run commercials for health insurance.

Companies collect millions of data points, recording practically anything imaginable. This wealth of information allows businesses to provide higher quality products to their customers while maximizing their profits. Despite these benefits of predictive modeling, potential privacy violations raise concerns. The rules for regulating the security of data warehouses—which preserve collected information in digital form on physical computer hard drives—are rather vague. According to the International Comparative Legal Guides' website page on data protection (2019), "the U.S. does not have a central data protection authority." Enforcement is inconsistent among the fifty states and depends on the stipulations of the relevant state statutes. Without well-defined rules and cohesive regulatory guidelines, proper data protection is hard to attain. And without proper protection, sensitive data are just waiting for malicious hackers to attack. Private personal details of real people are stored in these databases. An authoritative body such as the federal government, therefore, should require security standards to protect its citizens' privacy. Policymakers must realize the importance of this matter and start supporting consumers' privacy rights, following the examples of the European Union and the Philippines, which are discussed below.

This paper examines the potential ethical and economic concerns that predictive modeling in targeted advertising presents for American society today. In particular, it will focus on how Facebook technically violates its users' personal data rights. Notwithstanding, it will also articulate why Facebook is still a beneficial network. Too much restriction on Facebook's ability to use collected data for targeted ads could set a detrimental precedent for other social media

companies. When creating policy for better protection of individuals' privacy rights, there should be a balance between the interests of consumers in securing personal data and the interests of social media services in maintaining profitable operations.

Privacy Concerns with Facebook's Use of Personal Data

The term "big data" essentially refers to the accumulation of large amounts of data in data warehouses over time. In order to use this data to inform business decisions, data analysts "clean," or prepare, this raw data so that all entries in the dataset are readily usable. Then they manipulate the data through the use of programming languages such as R or SQL. Once the cleaning and intended transformations are complete, the analysts create charts and graphs that convey the relevant information in a meaningful way through programs like Data Studio or Tableau. Finally, utilizing the graphs created by the analysts, business executives can make well-informed decisions that are in the company's best interest. This process is roughly the same for all businesses selling any types of products or services.

One of the largest sources of big data stems from social media platforms. Social media influences the way people spend their everyday lives. Facebook is the largest and most well-known social media platform. On Facebook, users create an online social profile where they usually share interesting facts about their life and post pictures of themselves. People can interact with their friends and family, or even strangers, over the Internet through Facebook. Other popular social media platforms include Instagram, Twitter, and Snapchat. In a few easy steps, one can post pictures or life updates or share interesting articles on any of these platforms, where all of one's friends can instantly view them and have a quick interaction. Social media

encourages short—usually friendly—interactions with others, and it is a convenient way to stay connected with close friends and family on a regular basis. The ease of access to social media services facilitates their popularity. Almost everyone in America has a cellular device that supports these applications. According to Pew Research Center (2019), 81% of Americans own a smartphone. Adults can share a post while riding the bus or train and can reply to comments during breaks at work. These interactions only require one to two minutes of our attention at a time, and many people have made it a daily habit to check their Facebook or Instagram feeds.

In spite of the convenience, however, the amount of personal information that is shared publicly on these social media sites can be dangerous. People provide data such as their phone number, birthday, location, religious views, identity of family members, and life events on their Facebook profile. It is surprising how willing people are to share their personal information on the Internet, considering how easy it is for someone to take advantage of this knowledge for their own intentions, whether harmless or malicious. If a post or picture is public, any other Facebook user can access that information and manipulate it in any way they desire. For example, even if a user does not explicitly indicate which side of the political spectrum he or she falls on, Facebook can predict quite accurately that user's political affiliations based on what posts he or she likes or how that user responds to other people (Janjigian 2016). Some people may prefer to keep their political views private to avoid prejudgment and social discord. This is just one instance of how Facebook can take seemingly useless data and predict sensitive information through its specially crafted algorithms. The potential negative consequences of the Facebook predictive models are alarming.

Even if we assume that Facebook has no corrupt intentions with all the personal data it has collected, this does not mean that Facebook users are immune from privacy violations.

According to the Varonis company website (Sobers, 2020), “on March 21, 2019, Facebook admitted that since 2012 it has not properly secured the passwords of as many as 600 million users… On December 19, 2019, over 267 million Facebook usernames, Facebook IDs, and phone numbers were exposed.” These statistics are specific to Facebook, with more detailed information on data breaches available on their site. Once hackers have access to private Facebook datasets, they could steal people’s identities or credit card information. But malicious behavior does not even require access to these exact databases. Specifically, posting where you are and what you are doing is enough information for stalkers to find your location. Jennifer Golbeck and Matthew Mauriello (2016) from the University of Maryland recently published a study encompassing user understanding of what information Facebook can access. They surveyed 120 participants and sought both to discover the general public’s awareness of data privacy and to educate the subjects on the possible dangers of Facebook. Golbeck and Mauriello concluded that “people who are using apps are generally quite under-informed about what personal information they are handing over” (p. 8). After an initial survey, the study played a short horror film called “Take This Lollipop” for random individuals as an educational scare tactic. This film depicts the ease of determining one’s location from public information they post on Facebook. As a result of watching the film, almost all respondents reported a significant increase in concern for and awareness of privacy on Facebook. Potential malicious intent is not limited to the kind of cyberstalking discussed in Golbeck and Mauriello’s article. For example, a criminal can hypothetically plot a robbery with the help of Facebook. A felon might lurk around an expensive neighborhood and learn the names of its inhabitants by reading through the mail from their mailboxes. Then the criminal can look up their Facebook profiles online. If anyone

who lives in that neighborhood makes a post about going on vacation, this gives the criminal the perfect opportunity to rob that house.

Facebook is the model company to analyze when discussing big data and privacy rights. It is one of the most well-known companies on the planet; practically anyone who has access to the Internet has at the very least heard of Facebook. In fact, *Business Insider* (Reyes, 2019) states that Facebook has the largest number of users of any social media platform with 2.45 billion monthly active users. (According to Facebook, a monthly active user is defined as a single individual who has logged into his or her Facebook account at least once during the month.) Hosting 2.45 billion users indicates an enormous amount of personal data is at stake, implicating extraordinary potential for violations of privacy rights. American jurisprudence recognizes an actionable right to privacy. The right to privacy stems from the US Constitution. Although you will not find the word "privacy" written within its provisions, the United States Supreme Court has interpreted the Constitution to include a right to privacy. For the first time in 1965, the Court held in the landmark case of *Griswold v. Connecticut* that the right to privacy from governmental intrusion emanated from a "penumbra" of the First Amendment. Later in 1967, the Court held in *Katz v. United States* that constitutional protection extended to informational privacy when a person intended to keep certain information private, such as the contents of a phone conversation. While the constitutional right to privacy protects citizens against governmental invasion of privacy, statutes or common law can grant protection of individual privacy rights in the context of other private citizens or businesses. For example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 creates a right of privacy for medical information relayed to health care providers. Bodies of state common law, including Texas, historically acknowledge a private cause of action for the invasion of privacy (*Billings v. Atkins*, 1973).

Within the legal context, Facebook has already endured multiple challenges in the recent past. *The Street* (Fontana, 2018), which is a finance news website, lists sixteen different court cases against Facebook as of early 2018. Some experts have argued that Facebook violates the Civil Rights Act of 1964. For instance, in his article on advertising discrimination in the Northwestern University Law Review, Joseph Blass (2019) stated "though it is illegal to target job ads using statutorily defined protected characteristics (such as sex, race, age, and others), Facebook has recently faced criticism and legal action for targeting such ads in these exact ways" (p. 418). Facebook's machine learning algorithm sends specific job postings to different people based on their demographic and economic classifications. Title VII of the Civil Rights Act of 1964 states that employers cannot discriminate based on skin color or race. The algorithm clearly violates this legislation. However, it is unclear as to who the perpetrator is and whether legal action can be taken. Both the hiring company and Facebook could be violating Title VII. The hiring company wants to differentiate between potential new employees, and Facebook hosts the advertisement space and runs the targeting algorithm. Liability does not appear to fall directly onto one or the other. Additionally, the Civil Rights Act of 1964 (as well as other statutes) was written during a time period in which the legislative intent could not possibly have comprehended the technological capabilities of the future. Facebook is able to continue their actions because the laws have not been updated to address the Internet or data collection. This is one example of why new policies need to be created that specifically address data privacy on the Internet.

One of the most well-known privacy cases against Facebook is *Smith v. Facebook* in 2018. Winston Smith alleged that Facebook was tracking its users who access various healthcare websites. He claimed that it was an invasion of privacy to collect this biometric data. Allegedly,

Facebook placed cookies (which are essentially tiny strings of text stored on an Internet browser that connects information you give to a website to your personal computer) through its online advertisements that were able to track users as they accessed healthcare websites. For an example of how cookies are used, websites like Amazon can use these cookies to remember items that were in a previous shopping cart. Smith also alleged that Facebook collected sensitive information provided on these external healthcare sites and sold this personal data to third-party sources for profit. Facebook probably does not use this information for nefarious purposes, but the consequences of its practices could be detrimental for some people. A health insurance company that might purchase this information could raise rates for those specific individuals. Unfortunately for Smith, the District Court for the Northern District of California dismissed the case, stating that upon creating an account, users accept Facebook's terms of service, thereby giving Facebook the right to sell such data. The Facebook Terms of Service clearly states that "we collect information when you visit or use third-party websites and apps that use our services." Most users never read through the terms of service before creating an account. In fact, a "Deloitte survey found that over 90% of consumers accept legal terms and conditions without reading them" (Cakebread, 2017). The reason why consumers do not read the document before signing varies. One reason might be that the consumer simply does not want to spend the time necessary to read through its entirety. Even though users legally accept the terms of service, Facebook should not be allowed to carry out selling sensitive data, like the biometric data from the Smith case, in the first place. The uncontrolled disclosure of personal data has the capacity to render individuals susceptible to being taken advantage of, manipulated, or unfairly categorized. I discuss the conflict between Facebook and users' privacy violation claims later in the "Legal Discussion" section.

While judicial solutions may have been recent, user privacy on social media sites has been in danger for years. Action must be taken soon through spreading awareness about the risk of revealing too much personal information online or passing new federal legislation to protect consumers, or both. Although Facebook has increased its protection for user privacy in the past year, Blass claims that "systems such as Facebook's ad-placement algorithm are [still] likely to operate in a discriminatory fashion unless steps are actively taken to prevent them from doing so" (p. 420). Experts, such as Fred Cate (2006) from Indiana University, agree that existing principles or guidelines for data protection and privacy rights are not satisfactory. Because the technology industry changes rapidly, policymakers need to create comprehensive laws that adequately address this issue as soon as possible.

Big Data and How Facebook Operates

With the onslaught of big data, many businesses have expanded their corporate offices to include divisions for data strategy to analyze data for the purpose of improved business performance. Companies such as Facebook most likely desire to achieve maximum profitability with the least possible amount of effort. Such is the nature of most businesses operating in a capitalistic economy. Cutting edge practices include implementing these formal measures to enhance management decisions. Under this umbrella of strategic intelligence is a data department, which includes data analysis, data science, and data visualization. As noted in the previous section, data analysis is the process of cleansing raw data and aggregating the data together in a meaningful way. Data analysis is essentially a focused subset of the broader term, data science. And data visualization is the process of creating charts and graphs from the

analyzed data to aid executives in making better business decisions. This data could quite literally be anything, from what kind of car you drive, to how many pizzas you purchased last year, or to whose Facebook posts you liked last month.

Like corporate America, intelligence agencies in the federal government gather personal data, particularly since the passage of the Patriot Act (2001) in the post 9/11 world. Enacted to combat terrorism, the Patriot Act expanded government surveillance authority. Consequently, the United States government knows more about each individual citizen than one would think, which exemplifies the pervasiveness of data privacy invasion. It knows where you live, where you work, how much money you make, and possibly what you say during a cell phone call. Harry Pence (2015), professor at State University of New York at Oneonta, emphasizes the intrusiveness of this personal data collection: "The NSA [National Security Agency] is collecting almost 5 billion cell phone records a day to determine the locations of individuals and where they travel in the world even if they are not suspected of illegal activity… Even more troubling, it is illegal for the cell phone company to tell anyone they have received a subpoena of this type" (p. 257). Pence emphasizes the governmental intrusion the NSA committed when it took cell phone information from phone companies without the knowledge or consent of the consumer. Although Congress passed an act later in 2015 to end the massive collection of American cell phone data, government monitoring of your personal calls is a chilling thought. The vast majority of Americans do not realize that the government has recorded or tracked their calls, and most would likely consider this tracking an infringement of their privacy rights. Even if you are not bothered by the government recording your phone activity, it is a matter of principle. If the government has been allowed to collect and use this information at its own discretion now, further invasion of privacy may subtly increase in the future to the point that individual rights are completely

eroded. While governmental agencies such as the NSA collected our data under the guise of national security, most international corporations like Facebook assemble billions of data points a day to maximize company profits. Although the type of data collected and the purpose of the collection is different, the concept is still the same with Facebook.

Before discerning whether or not this intrusive data accumulation violates any privacy rights that American citizens may or may not have, it is important to understand how Facebook actually operates and makes a profit. Facebook is a free service that is able to return a profit by selling screen space on its website or application to other businesses. These companies purchase this space to advertise their own product or service to Facebook users. Tom Funk (2012), an expert on social media marketing, devotes an entire chapter of his book to Facebook advertising. (Although Funk's book was written in the last decade, the information about how Facebook works is still accurate as of early 2020.) How much money Facebook charges to advertise on its platform is measured in cost per clicks (CPC) or cost per thousand views (CPM). A click is defined as when a user selects the ad with his or her computer mouse icon, and a view is when an ad is visible on a user's screen. There are various types of advertisements, each with a different cost. The price typically depends on how likely a user interaction with the ad leads to a sale. Funk claims that "the average CPC for ads leading off Facebook was $1.08, compared with the $0.70 for on-Facebook entities" (p. 79). For reference, an ad leading off Facebook is an ad that redirects the user to a new website and an on-Facebook entity is an ad that keeps the user on Facebook's website when clicked. When purchasing an ad space on Facebook, the advertisers indicate how long they wish the ad to remain on Facebook. Once that time is passed, Facebook calculates the total cost and sends a bill to the advertiser. With a 2.45 billion monthly user pool

(Reyes, 2019), it can be expensive to advertise on Facebook because the demand for ad space heavily outweighs the supply.

Because advertising space works like any other open market system subject to the law of supply and demand, Facebook cannot simply increase its profits by continuing to raise the cost per click price higher and higher. At some price threshold, companies will simply stop buying ads from Facebook because the cost would outweigh the benefit. Therefore, in order to increase profitability of the company, Facebook uses targeted advertising as a way to boost the likelihood of users to click on an ad. Targeted advertising is a tactic that aggregates large amounts of preferential and demographic data to determine which users are more likely to click on a particular ad. This is exactly why the ads that you see on your Facebook page can be completely different from the ads that your friends see on their pages. Facebook has created a complex analysis algorithm that takes personal information such as age, ethnicity, socioeconomic status, and even what posts you have liked in the past to predict your unique preferences. For example, this algorithm can predict with high accuracy your approximate yearly income from your pictures, posts, and the way you chat or interact with your Facebook friends online (Matz et al., 2019).

The term for such a complex algorithm is predictive modeling. Predictive modeling is an increasingly used statistical tactic that analyzes varying information and forecasts the future. Most notably, the insurance industry makes use of predictive modeling on a daily basis. This kind of modeling predicts the future based on statistics from past collected data. Insurance company use of predictive modeling contributes to the fluctuation of insurance rates among populations. An auto insurance company will determine that if you are in a car accident, the rates you pay should increase because you are now statistically more likely to become involved in

another car accident. Similarly, if both your parents have histories of heart problems, health insurance rates may increase because of the likelihood you will inherit their heart issues. The fact that health insurers can raise rates based upon knowledge of your family's medical history raises some ethical concerns. The problem with forecasting the future is that most—if not all—predictions are not 100% certain. For example, even if a person is genetically more likely to have heart problems, that does not mean he or she will actually develop them. The insurance company perceives an increased risk of higher claims and passes this anticipated expense on to its customer through higher premiums, even though the insured may never submit a claim at all. While the person whose parents both have heart disease is statistically more likely to have issues in the future, a propensity for a condition does not mean actually suffering from the condition. That person might follow a healthy regimen unlike their parents and, therefore, never have heart problems, so it is unfair to incorrectly assume future consequences merely based upon heredity. A more appropriate application of predictive modeling is to use such algorithms to make accurate assumptions about unknown facts in the present.

Sandra Matz (2019) and her colleagues conducted a study to show the power of predictive modeling in Facebook by creating their own model. They took 7,180 participants and asked to thoroughly examine their public Facebook profiles. After collecting all the necessary personal data, they plugged this data into their carefully crafted prediction model. By only looking at Facebook likes, status updates, and profile demographics, Matz and her colleagues were able to predict the participant's income level with 43% accuracy. If a small team of university professors can create a model with relatively high accuracy using minimal funds, a company like Facebook, worth over half a trillion dollars (Macrotrends, n.d.), could certainly create a better model to predict your annual salary. Even if you have never disclosed your

income level in public, Facebook likely can determine it. Again, the main problem with Facebook being able to calculate your annual salary is a matter of principle. This is just one example of the potential for overreaching implicated by predictive modeling. Focusing on a different data point would likely result in similar encroachment. The Matz (2019) study concludes by acknowledging: "it becomes paramount to ensure that these algorithms do not discriminate against specific subpopulations… Our findings demonstrate the need for ethical guidelines for predictive technologies, as well as regulations on a policy level" (p. 10). Notably, they emphasize how Facebook has the capability to potentially abuse predictive modeling and call on policymakers to protect user rights from discrimination.

In addition to its use of predictive modeling, another ethical issue concerning Facebook's personal data collection is targeted advertising. Such a strategy openly differentiates between users based on their age, race, ethnicity, and political standing, pushing the boundaries of federal discrimination law. One legal challenge in November 2019 involved a class action lawsuit for gender and age discrimination. In *Opiotennione et al. v. Facebook Inc.*, a 54-year-old woman named Neutah Opiotennione sued Facebook for discriminating against females and elderly people in their financial services ads. Supposedly, such advertisements are targeted towards younger people and men because they are more likely to interact with the ads and use financial services. Because the price of advertising is heavily dependent on the number of viewers, advertisers want to publish their ad only to the consumers they deem most likely to do business with their company. Consequently, Facebook accommodates their paying clients and participates in this targeting scheme for profit. The advertisements in the Opiotennione case purposely discriminated against users based on gender and age for financial service opportunities, which violates Title VII of the Civil Rights Act of 1964. In another lawsuit, Facebook clashed with the

United States government over the housing sector. The Department of Housing and Urban Development (HUD) sued Facebook in March 2019 for violation of the Fair Housing Act of 1968. HUD argues that individuals were being discriminated against because of their religion, family status, and race. Specifically, the plaintiff claimed that Facebook encourages housing advertisers to exclude particular groups of people from receiving their ads (Corbin, 2019). Although the case is still pending with no final ruling, this discriminatory behavior from Facebook can be interpreted as a violation of individual rights. Policymakers need to address these blatant indiscretions targeted advertising can cause with data privacy. Unfortunately, this kind of bias is not unique to Facebook. Other social media sites—and all other media outlets for that matter—engage in similar advertising activities. This is why America needs sweeping data privacy reform across all industries.

A further problem with Facebook is the availability of personal information to any public Facebook user. This is more of an issue with the carelessness of naïve users rather than with the company itself. However, Facebook's privacy settings for each user profile contribute to the situation. The default privacy settings for a new Facebook profile have maximum publicity, meaning everything you post and like on Facebook is public for all users to see (including people who are not your friends). Updating your geolocation online could lead to adverse consequences. Referring back to an example from the previous section, if you frequently post about where you commonly go out to eat and work, an intelligent stranger could determine the general location of your house. Then, when you make a post saying that you are on a family vacation out of state, that stranger has the opportunity to rob your house while everyone is away. Of course this example assumes that you share enough information about yourself and your location, and that someone is smart enough to figure out this plan of attack. But the possibility exists, and there is

potential for malicious use of the Internet to result in harm. Researchers Phillip Nyoni and Mthulisi Velempini (2018) conducted a study on privacy awareness among Facebook users. The experiment tracked 357 people and determined the privacy measures (if any) that people take to protect themselves on Facebook by analyzing how publicly open each participant was with their personal information. The study found that "when [most] users share personal data, they do so without an understanding of the risks involved. They assume that Facebook is a trusted computing platform, but that is not always the case. For example, hackers can create false accounts or clone user accounts to steal personal data" (p. 27). Nyoni and Velempini also found that around 33% of participants allowed Facebook full access to their personal data, while 67% only allowed partial access. Of this 67%, most did not realize that their posts and profile were still accessible to the public domain. Their information is readily available for any Facebook user to see.

Many people do not realize the negative consequences of having their personal information freely accessible. Having your data stolen by another Facebook user can be dangerous. Recall Golbeck and Mauriello's (2016) study illustrating this danger in their interactive horror film called "Take This Lollipop." The short movie took Facebook information from the individual participant and incorporated it into the story in which a psychotic stalker used Facebook to find a person's location. Although Golbeck and Mauriello's case might be extreme, the possibility of disturbed people using Facebook to stalk others is a legitimate concern.

While creating a user profile is free of charge, Facebook is technically not free to use. Users pay for social media services through their data. Jacob Johanssen (2018) from the University of Westminster in London wrote an article about his unique perspective. He argues

that Facebook is a game—because it can be enjoyable and entertaining—where the goal is to accumulate as many likes and comments on your posts as possible. Then he elaborates on this topic and theorizes that Facebook takes advantage of its users' data as a form of labor. Johanssen states that online activity creates social networks and relations, location data, browsing data, etc. This activity is both fun and work at the same time—play labor. This "play labor" is a data commodity that Facebook sells to advertising clients (p. 1205). To contextualize the vast amount of data that Facebook accumulates, recall the predicting income study from above. Matz (2019) and her colleagues provide some useful statistics: "On Facebook alone, there are more than 510,000 comments posted, 293,000 statuses updated, and 136,000 photos uploaded every minute" (p. 2). As Johanssen pointed out, Facebook sells this massive amount of data to advertisers for profit and uses the data itself in its targeted advertising algorithm. This idea of "play labor" poses the question of the monetary value of Facebook user data.

Professors Gianclaudio Malgieri and Bart Custers (2018) conducted extensive research about how to accurately price privacy. They claim that personal data represent monetary value in the data-driven economy and are often considered a form of payment for the free digital services that companies like Facebook provide (p. 289). Through examination of practical data monetization models, they argue that people should at least be informed of the fiscal value of their data. Malgieri and Custers acknowledge that actually quantifying this value is difficult and who does the quantifying can create bias. For example, if Facebook is allowed to quantify the value of the data it collects, it may undervalue that data to create a larger profit margin. Although there is no uniformly accepted calculation, Malgieri and Custers provide a few example prices to give a better understanding of the approximate value. Specifically, they claim a person's demographical information of age and gender is valued around five cents, but information

regarding potential auto buyers (such as previous insurance claims or speeding tickets) is worth 21 cents. The type of data disclosed and what company is purchasing the data will influence the price. A few cents might seem insignificant, but data purchasers buy in large quantities, in the hundreds of thousands, or millions. Taking Malgieri's and Custer's price of personal data into account, monetary value can be assigned to personal data. The value for most types of data, however, is quite small. If demographic data such as age and gender are only worth around five cents, most users would likely consider the service that Facebook provides to be worth more than such a negligible usage fee.

No discussion of massive amounts of valuable data is complete without mention of the attraction of hackers. The data that Facebook collects from each of its users have to be stored somewhere. Data warehouses in cyberspace hold this information for easy access by data analyst teams. Think of data hackers like malware. Computer viruses attack hard drives and install malicious software to ruin the computer. Real life data hackers exist as well and wish to break into these cyber warehouses to use the personal information for profit or other selfish intentions. To contextualize the prevalence of data breaches, in the first half of 2019 alone, over 3,800 data breaches were publicly reported (Winder, 2019). Also in 2019, large corporations like Capital One, State Farm, and Quest Diagnostics were hacked; hundreds of millions of sensitive data records were stolen from their customers (Henriquez, 2019). In July of 2018, British Airways was fined 183 million British pounds for insufficient data security after 500,000 customers suffered from a web skimming attack, which involved stolen credit card information from an online payment page (Sweney, 2019). In 2018, the personal data of over 50 million Facebook accounts were exposed in a large-scale security breach (Perez & Whittaker, 2018). This hurts the customers because their bank account, auto, and health information was at the mercy of unknown

individuals. These breaches also damage the companies because of the loss of clientele trust and detrimental financial implications. A business must inform its customers of the situation, and in the case of a bank, thousands of credit cards need to be cancelled and replaced to prevent any harm to assets. These attacks can cost millions of dollars in damages and severely impair trust with customers. Consumers can lose faith in a company because if a data breach happens once, it is likely to happen again unless drastic security enhancements occur.

Despite these alarming concerns, people still choose to use Facebook. For many, the positive benefits of staying socially connected online outweigh the potential negatives listed above. Most others are simply unaware of these dangers. Because a service like Facebook is so widely used on a daily basis by Americans, it is necessary for an institution to protect users' personal data. If Facebook itself will not enhance security, then the responsibility to protect consumers falls on the state and federal governments. Other nations around the world have stepped in the right direction. The federal government should follow suit and both acknowledge and preserve the right to data privacy protection.

Legal Discussion

Despite the concerning problems with Facebook and data privacy, the United States government does not have a comprehensive legislative scheme protecting citizens' data privacy. Exactly half of the fifty states do have enforceable laws, but the legislation in place is not complete and differs from state to state. For example, Maine's Act to Protect the Privacy of Online Customer Information (2019) requires consumers to opt-in to having their data collected while California's Consumer Privacy Act (2018) requires companies to offer an opt-out option. These subtle differences in state statutes affect not only customers; they can also create a

compliance nightmare for businesses. Cybersecurity expert Charlotte Tschider (2015) substantiates this point, explaining that "without consistency between states, it may be cost-prohibitive for many businesses to comply with individual state mandates" (p. 65). The disparity between the laws of each state creates uncertainty as to the best course of action to be taken at the federal level.

The fact that the Internet transcends state boundaries and that Facebook has such a massive impact on our society demands a comprehensive federal law. Let us assume that all fifty states had enforceable laws. There would likely be differences between the statutory language in at least a few states in the absence of a uniform code. Running ads on Facebook suddenly becomes complicated because the advertisements must adhere to individual states' laws. Given the complexity of conflicting laws, Facebook's compliance with these state laws might indirectly break the very laws they attempt to follow. The following example is hypothetical and mentions random states to exemplify the point. If Tennessee and Maine passed legislation stating that Facebook may not use any personal information in targeting their advertisements, Facebook is forced to withdraw all advertising in Tennessee and Maine. Because targeted advertising increases profitability over non-targeted advertising, Facebook would send their ads to all states except Tennessee and Maine. However, by excluding Tennessee and Maine users, Facebook indirectly uses the geolocation of the user and violates the prohibitions in Tennessee and Maine that they were trying to avoid. Even if all fifty states had roughly the same enforceable data privacy legislation, it would still be less efficient than federal legislation. In addition to one comprehensive federal statute providing uniform protection, future amendments and updates to the legislation would be quicker than the varied schedules of the fifty state legislatures. Moreover, if there is a need for judicial interpretation of the law, the federal court system could

consistently follow federal precedent as opposed to a possible piecemeal approach from different judges in all of the states. From these simple hypothetical situations, it is clear that a federal mandate on data privacy protection is a better alternative than individual state solutions.

Although the United States government has no law specific to data privacy protection for all citizens, a few less authoritative and precise rules and recommendations do exist. The least useful and most outdated solution to data privacy problems is the Federal Trade Commission's fair information practice principles (FIPPs) from 1973. These principles stipulate that consumers must be made aware that their information is being collected, give consent, and be able to view the data if requested. The data must be authentic and secure, and there must be some form of regulation. The principles encourage self-regulation, but allowing companies to control their own data privacy requirements is an invitation to noncompliance. Despite providing groundwork for many laws such as the Right to Financial Privacy Act (1978) or the Video Privacy Protection Act (1988), the FIPPs are simply recommendations and do not confer legal authority to regulate data privacy of specific platforms like the Internet. Furthermore, these principles are close to fifty years old, making them largely obsolete for modern standards given the exponential developments in data collection and usage (Solove, 2018). Industries constantly evolve with new technological advances, and successful businesses are quick to adopt the new changes. Policymakers need to create legislation that not only accounts for current privacy issues but also anticipates how innovative measures might further implicate data protection.

Currently, the only federal law related to online privacy is the Children's Online Privacy Protection Act of 1998 (COPPA). This statute restricts the collection of any personal information on a minor 13 years old or younger for any purposes. Because the age requirement to create a Facebook profile is 13 years old, Facebook is unaffected by the act. Although the statute serves a

valid purpose in protecting children's privacy, its implementation illustrates how data privacy laws have the potential to overly restrict companies. COPPA is enforceable by the FTC, which has pursued multiple large corporations violating the act. For example, YouTube was fined approximately $170 million in late 2019 for tracking minor viewership for the purpose of creating more effective targeted advertising opportunities (Federal Trade Commission, 2019). The FTC is clearly vigilant in protecting American children's privacy. However, the settlement has unintentionally created some negative consequences for the YouTube creator community (Spangler, 2019). Part of the FTC mandated reparations called for YouTube channels to be marked as "child-oriented" or not, but the definition of a "child-oriented" video is subjective and controversial. If a content creator marks his channel differently than the YouTube machine learning algorithm marks his channel, that creator can be fined $42,000 per video. This outcome could force unsuspecting YouTube creators to bankruptcy or lifetime debt to the FTC. Although this has not yet happened to any creator, YouTube's sudden implementation of the COPPA restrictions created an unsettling scare to those whose livelihoods are in jeopardy. Such a law harms individual content creators disproportionately more than it harms the actual company running the advertisements in the first place. A $170 million fine to a multi-billion dollar company is minor compared to a $42,000 per video penalty to one person. Just one of these $42,000 fines could ruin someone's financial standing. Although COPPA protects data privacy for minors, it can negatively impact the lives of innocent entrepreneurs. This is just one illustration of why policymakers need to take extra precaution to consider all interests when creating a new comprehensive federal data privacy law.

At the state level, most recently California passed the California Consumer Privacy Act (CCPA) in 2018. According to this statute, any Californian citizen has the right to know what

personal data is being collected and the right to request that the company stop selling their data. The implications of this new law are still in the infantile stages. However, it is important to note that because California is the largest state by population, most online businesses must comply with this law. Other states have begun the trek towards better data privacy protection. Also in 2018, Vermont passed a law similar to the CCPA under the Vermont Statutes Online, Title 9, Chapter 62, Subchapter 2. This statute mandates that all data brokers must disclose to individuals what data is collected and provide the option to deny permission. Maine and Nevada adopted new statutes in 2019, yet these statutes are not as broad as the CCPA. Nevada's law amends Chapter 603A of the Nevada Revised Statutes but only applies to data collected from consumers through the Internet. Maine's Act to Protect the Privacy of Online Customer Information, which goes into effect in July 2020, is limited to internet service providers. Other states have proposed legislation without success. States like Connecticut and Florida have attempted to pass data privacy bills in recent years, yet they have failed to become enforceable laws because the bills did not receive enough support. If the statutory schemes operating in California and Vermont prove successful, the federal government should follow their examples. The United States government should take a definitive stance on the issue to preempt the variable processes of state legislation and create legal parameters for Facebook and other similar businesses.

Unlike the United States, other influential countries have already taken considerable actions to defend their citizens' privacy rights. Europe takes the lead with the most comprehensive data protection laws. The European Union adopted the General Data Protection Regulation (GDPR) in 2016. This regulation requires businesses to implement high-quality personal data protection and security measures. The data collectors must disclose the purpose for any collection and state how long the information will be retained. The collectors also have to

notify consumers if they are transferring data outside of the European Union. A business that frequently handles personal data must staff a data protection officer whose sole responsibility is to determine if the business complies with GDPR standards. Most significantly, all people must consent to their data being collected and have the right to revoke consent without losing access to that service. Supposedly, Facebook has agreed to follow GDPR privacy standards in every country around the world. Consequently, Facebook attempted to receive permission for its data collection from users rather than reducing its collection. But it crafted the agreements to make it much more difficult to opt out (Solon, 2018). Hence, despite the success of the GDPR, Congress should evaluate how it could be improved upon in American legislation. In short, the GDPR is similar to—but stronger than—the CCPA and should be the primary model for the United States.

Malgieri and Custers (2018), who co-authored the pricing privacy article discussed above, summarize the GDPR: "If a data subject is asked to consent to the processing of personal data (which is not necessary for the performance of that contract) in order to have access to a service or for the performance of a contract, it is highly probable that his consent is not 'free', and so it is not valid under the GDPR" (p. 298). In this way and in many others, dozens of companies have already violated the GDPR and have had to pay significant fines. Whether or not companies are purposefully breaking laws like the GDPR, it is clear that personal data collection is so important for business profits that large corporations are willing to ignore the guidelines that the GDPR has outlined.

The European Union is not the only large foreign entity that has provided data privacy protection for its citizens. For instance, Russia acknowledges the importance of this issue. Anna Zharova and Vladimir Elin (2017) from the National Research University Higher School of Economics in Moscow wrote an article on data security from their home country's perspective.

According to Zharova and Elin, “only the person has the right to determine what kind of information relates to his private life and must remain a secret. Therefore the collection, storage, use and dissemination of such information is not permitted without the consent of the [individual] person, as required by the Russian Federation Constitution” (p. 488). However, Russian citizens give consent to Facebook when they sign its user agreement. Although Russian law does protect personal data, its statutes were adopted more than a decade ago and should be amended to address more current practices of data collection. But at least Russia has some data privacy legislation, unlike the United States. In their conclusion, the Russian co-authors call for updated and more specific legislation so that companies cannot easily find loopholes, as they have done so far.

In comparison to Russia, the Philippines has privacy laws that more adequately protect its citizens. Marck Joseph Macaraeg (2017) from Ateneo de Manila University School of Law wrote a paper that encompasses the entire status of data privacy in the Philippines. Macaraeg invokes his country’s Constitution when discussing the importance of the right to privacy, stating that “it is expressly recognized in Section 3(I) of the Bill of Rights: The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by the law” (p. 232). Because this right is so essential to the Philippines culture, the government passed the Data Privacy Act (DPA) of 2012, which directly addressed concerns with personal data security. Citizens must be informed when their data is being collected and must be told for what purpose. They also have the right to request data collectors to immediately stop processing their individual data. In short, Filipinos have rights similar to those granted in the GDPR from the European Union.

Having analyzed the data privacy laws of other prominent countries around the world, it is clear that the United States federal government should look to the success of the GDPR from the European Union, or even the Data Privacy Act from the Philippines, for guidance when formulating a comprehensive data privacy law. The government should first and foremost protect its citizens' rights, but it should also take into consideration the rights of companies to create wealth. Legal structure is necessary to prevent companies like Facebook from taking full advantage of unsuspecting American consumers. But such action must be done within reason, balancing individual rights with the financial interests of the companies. Tighter restrictions on data collection and usage for high profiles companies like Facebook might only cause a dent in corporate profits. Large businesses like Facebook have shown resiliency in the past when it comes to adjusting policies to abide by federal legislation. But such harsh constraints might have extreme consequences for smaller businesses or other people merely interested in using data-driven platforms for innocent purposes.

Implications of Heavy Restrictions on Data Collection

When considering the most effective method to implement a new data privacy law, it is important to study historical precedence. Human history has been known to follow patterns and repeat itself across millennia. By looking into the past to understand our faults and shortcomings, we can better prepare ourselves for the future. In this instance, policymakers should consider any past failures (such as the unenforceable fair information practice principles (FIPPs) from 1973). Although data privacy legislation is in its infancy stage, there are recent cases of success from which wisdom can be drawn, whether from domestic state laws or foreign policies, as discussed in the previous section. The United States government should consider all of these examples and

modify them to protect the interests of both consumers and businesses, and to minimize implementation challenges.

Facebook has clearly pushed the ethical data privacy boundaries, and, in doing so, has been sued frequently for violating a wide range of possible privacy rights. But Facebook has a right to conduct its business and contribute to our national economy. As of March 2020, the CEO of Facebook, Mark Zuckerberg, has a net worth of $82.6 billion (Hoffower, 2020). His company has its own right to focus on maximizing corporate profit. While Facebook does actively try to improve upon its privacy policy and other services with user feedback (through volunteer online surveys or focus groups), the consumers could use more education about their privacy rights. A privacy policy in favor of the user—no matter how beneficial Facebook claims it to be—does no good if the users never read or understand the policy. Nyoni and Velempini (2018), who studied user awareness of privacy on Facebook, found that "the privacy policy is long and written in technical language which is not easily understood by most users. The policy highlights that privacy is a shared responsibility and users need to be proactive as well" (p. 30). They mention that Facebook users do not see this as a contract and fail to update their own privacy settings to better secure personal data. According to the responses from their survey, most Facebook users assume that Facebook takes full responsibility for their privacy. In actuality, the user and Facebook are equally responsible (as mentioned in above). When creating a new Facebook account, the default privacy settings are set to maximum publicity, meaning that all the information, photographs, and comments posted on the website can be seen by every Facebook user—even users who are not your registered "friends." From this discovery in the fine print of the privacy policy, it is clear that Facebook is not completely at fault in supposed privacy violations. Even though Facebook should set the default settings to minimum publicity for the

benefit of consumers, the user is also held responsible for how much personal information they reveal online. And remember that the user legally gave Facebook permission to collect and use his data when he agreed to the terms of use and service.

This is why the terms of use and service for Facebook—as well as the privacy policy—are important documents to keep in mind when considering how to create a new federal data privacy law. Although users are required to read and agree to the privacy policy when creating a new Facebook account, an overwhelming majority of Facebook users never read the fine print. Recall the Deloitte survey that concluded around 90% of consumers do not read terms and conditions. They simply scroll down to click the accept and continue button. Either people have no interest or time to read the document, or they do not care if the information they share online is taken by someone else. Most of the time, Facebook is within their rights to do what they please with the data they receive. Users sign away these rights when they click that "accept" icon. Golbeck and Mauriello (2016) found convincing evidence that "users are concerned about privacy on Facebook, particularly with respect to the information apps can access. At the same time, users were generally under-informed about what information Facebook apps can access" (p. 12). Yes, there is a clear concern about data privacy. But the users are not educated enough on the subject to fully understand what is happening because they simply have not spent the time to learn about the situation.

There are two definite solutions to this problem of ill-informed users. The obvious, yet least appealing option, is for users to just read the fine print of the document they are signing. Another option is to educate all Facebook users on Facebook data privacy in simpler terms. Ideally, this education could come through schools and social groups. Even just advising caution when posting sensitive information online can go a long way. Or teaching users about their

privacy options through a simple online tutorial could be helpful. Facebook users can make their account much more secure from unwanted visitors by taking a few short minutes to navigate to the privacy settings page and update their settings from “public” to “friends only.” Even though Facebook still collects and sells this data, users would be protected from strangers.

It is in the best interest of the American consumer to assume the worst-case scenario for data privacy breaches or misuse. While Facebook has its own company profit in its best interest, the typical Facebook user is ill-informed about data privacy, as shown in the study by the Golbeck and Mauriello (2016). Under these circumstances the federal government should step in for the safety of its citizens. Unenforceable guidelines, like the United States has implemented in the past, remain useless. We need an enforceable law encompassing data privacy for all social media applications—not just for Facebook.

The government, however, should not completely disregard the interests of Facebook in crafting a new data privacy statute. Social media services such as Facebook, Twitter, and Instagram are currently free for every user. As discussed above, a large portion of corporate profits come from advertising revenue. If the advertising abilities of such companies were severely restricted, significant and unwanted repercussions could result. Less advertising leads to a decrease in profits, which would drive the companies to find a new source of revenue. One way that Facebook could make up for this profit loss is to require its users to pay a subscription fee. There is no academic research on the implications of making Facebook a paid service, but most likely the number of Facebook accounts would surely decrease. Hence, a restriction on data collection practices could adversely affect the American consumer, which would counteract the original intentions to benefit the individual.

Although there is minimal research to back up these assumptions about potential negative impact for social media platforms, some does exist. Attorney Lauren Stewart is one of the few who directly addresses the balance between the need for data privacy protection and the right of businesses to use data collection for profit. She claims that "overregulation … risks disincentivizing businesses from implementing potentially beneficial technology into their products and services" (p. 386). Like this thesis, Stewart calls on the federal government to create a new data privacy law in order to eliminate consistency issues with separate state statutes. This new federal law needs to address the data privacy concerns of American consumers. But it must do so with the business point-of-view in mind. Hindering corporations in our economy can and will indirectly affect the consumers that such a law intends to protect. Policymakers must proceed with caution to maintain a balance. At the very least, the United States should start by implementing a law similar to the GDPR. Expanding further, the US law should require companies like Facebook to be more transparent with data collection methods and third party data purchasers. Specifically, an obvious and concise disclaimer (simple and short enough for the average consumer) should visibly pop up on the screen when users log in. By adopting regulations that value both individual privacy rights and companies that collect their personal data, the government will provide industries with the opportunity to serve their customers in an ethical manner.

Limitations and Potential Solutions

This section addresses the limitations of the proposed solution and clarifies the primary need for both data privacy education and federal legislation. Although the referenced studies indicate many people are concerned with the security of their personal data, other people might

not oppose Facebook collecting and using their data. Some might not understand why the collection and use of their data is problematic. In fact, they might encourage it because the predictive modeling algorithms would provide them with advertisements that they might want to see. Just as discerning the thoughts of individual users is virtually impossible, knowing the true intentions of Facebook is difficult. It is unfair to assume that it has inherently malicious intent with the personal data it collects and sells. Also the assumption that Facebook stalkers are commonplace, like the one in the "Take this Lollipop" short film (Golbeck & Mauriello, 2016), is implausible. However, it is better to assume the worst possible scenario rather than to assume that Facebook is solely focused on consumers' safety and privacy.

Another limitation to the policy-making solution is how to improve the security of data warehouses. Even if Facebook has the best possible security, some data hackers could still breach the firewall protection, as they have in the past. As noted above, at least 267 million usernames, IDs, and phone numbers were prone to being leaked during a Facebook data breach in 2019 (Sobers, 2020). Companies should not have the right to collect data if it cannot be securely stored. However, cyber security and technological firewall protections can experience breaches and their technicalities and legal implications are beyond the scope of this thesis.

As for actions consumers can take to protect their data privacy rights with regard to Facebook—and other social media sites—changing the privacy settings on their accounts is a good start. Users can also be more cautious with what information they share online and always think of the potential consequences of their actions. Alyson Young and Anabel Quan-Haase (2013) conducted a survey for college students to better understand what is called the "privacy paradox" on Facebook. They state that the privacy paradox refers to "a sharp disconnect between the concern people express and their willingness to disclose personal information" (p. 480).

Although students from their survey responded with concern about Facebook collecting their data, the same students openly shared their information and photographs with Facebook as if they had forgotten about the concern they had so recently displayed. Young and Quan-Haase conclude by calling upon policymakers to increase the clarity of what kind of data are collected, how the data are aggregated, and how the data are utilized for certain Facebook features such as advertisements (p. 494). This increase in clarity can be attained through legislation that requires Facebook to modify its practices and to provide explicit details about its data collection. Law professor Ari Waldman (2016) concurs, referencing how the "FTC recommends that before … apps access sensitive information, they should provide concurrent disclosures of the impending data use and 'obtain affirmative express consent' from users" (p. 207). His notation makes logical sense because in order for consent to be truly informed, the user should have simultaneous access to an understanding of the scope of that consent. Consumers might have long forgotten the explicit verbiage of the terms and services page that they may—or may not—have read upon creating a Facebook account.

As a final emphasis, awareness of data privacy intrusion must be increased. An academic study exhibited the success of privacy awareness campaigns. Meredydd Williams, Sadie Creese, and Jason Nurse (2019), who are computer science professors from the University of Oxford and the University of Kent, administered a survey to college students to collect data on privacy protection behaviors. They created an interactive smartwatch game that educated the participants about sound privacy behaviors on the Internet. Some prudent behaviors involved creating new passwords every month or disabling GPS (Global Positioning System) tracking when you are not using the application. Williams, Creese, and Nurse concluded that once their participants were well-informed about optimal privacy protection practices, most actively carried out these

practices in their own lives after the study period. The remaining participants who did not carry out these practices had actively made the choice to sacrifice their data for convenience (p. 50). Although the success rate was not 100%, at least all the participants had been educated about the risks and were able to make their own choices. The positive acceptance of this awareness campaign for privacy protection on a small scale indicates that a large-scale awareness campaign could be just as successful. If more Americans understand data privacy risks, more will start to adopt practices to protect themselves and educate others.

With the authority to regulate corporate behavior, policymakers hold the most power over the protection of data privacy rights. Legislators need to become educated through the efforts of a data privacy protection task force. Understanding both the interests of the consumer in privacy and the ability of the companies to operate profitability while providing free services will help legislators to make well-informed decisions. Data privacy laws are needed as soon as possible to prevent further erosion of consumer rights. The longer policymakers delay, more companies will be allowed to increasingly infringe upon the privacy rights of American citizens by pushing that invisible line further and further for their own benefit. At some point, such legislation would receive too much pushback from business without enough support for individual rights (Rojas, 2018). Although an unlikely proposition, there is potential for our nation to develop into a dystopian society with zero privacy where the government—and businesses—can see everything its citizens say and do. Edisa González and Ricardo Vizcaíno-Laorga (2018) address the extent to which technological innovation could adversely impact social integrity. In their exploration of recent communication technologies, they assert: “Taken to the extreme, [connectivity growth] could place us in a scenario in which we could talk about ‘technophobic dystopias,’ where technology would lead us to a situation that we really do not want to reach” (pg. 300). If societies

fail to remain mindful of individual privacy rights, then perhaps George Orwell's famous dystopian novel, *Nineteen Eighty-Four*, will be reclassified from science fiction to historical fiction. Congress has the opportunity to assure this does not happen in the United States.

Conclusion

Understandably, minimizing costs and maximizing revenue are the key goals of any successful company in a market economy. Because of growing technological advances in data science, businesses are adapting at a rapid pace in order to optimize corporate profits. Data analysis tactics and predictive modeling algorithms that drive the modern economy, therefore, are here to stay. Along with big data, however, comes the issue of the invasion of privacy. That is why the government must protect consumer rights and take action on data privacy.

The United States lags behind other countries in data privacy policies with no comprehensive, enforceable law that specifically addresses data collection and usage on the Internet. Although some states have addressed these privacy concerns, others have not. In order to facilitate national coverage and eliminate discrepancies between state laws, the federal government should enact data privacy legislation to protect personal data from potential abuse.

As lawmakers begin to formulate policy, it is essential that they value the importance of data privacy for individual users. Equally—if not more—important, however, policymakers must understand the complete picture behind data collection and usage. Too much constraint can have significant negative impact on companies. Moreover, heavy restrictions could create negative consequences that indirectly fall upon the consumer. A delicate balance should be reached between the data privacy of the individual consumer and industry's ability to exact a profit from providing services to the consumer.

Optimally, the United States needs to implement a law resembling the European Union's GDPR and build upon its foundations to create a regulatory scheme tailored to American interests. The law should demand heightened transparency with data collection practices. A simple protocol to include is mandating that companies provide a visible, understandable disclaimer—separate from the terms of service agreement—disclosing this information. As an enforcement mechanism, the FTC could impose heavy fines on companies that fail to comply. Cybersecurity analysts and social media experts should be consulted in conducting additional research regarding the best approach to undertake.

Because legislative development is a lengthy process, American consumers should educate themselves today on the potential dangers of personal data misusage and take appropriate action. Each Facebook user can update their privacy settings for their accounts. Social media companies as well as other Internet companies can offer simple guidance for consumers to make more informed choices. Schools can teach students about data privacy and the use of the Internet or social media platforms. Non-profit organizations can publicize the importance of taking precautions with sharing personal data. The more awareness spreads, the less likely individual privacy rights will be violated.

References

Billings v. Atkins, 489 S.W.2d 858, 860 (Tex. 1973)

Blass, J. (2019). Algorithmic Advertising Discrimination. *Northwestern University Law Review*, *114*(2), 415–467.

Cakebread, C. (2017, November 15). You're not alone, no one reads terms of service agreements. Retrieved from https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11

Cate, F. H. (2006). The Failure of Fair Information Practice Principles . In *Consumer Protection in the Age of the Information Economy*. doi: https://doi.org/10.4324/9781315573717

Corbin, K. (2019, March 28). HUD Is Suing Facebook For Housing Discrimination. Retrieved from https://www.forbes.com/sites/kennethcorbin/2019/03/28/hud-suing-facebook-for-housing-discrimination/#6fb10ef67547

de Luce, I. (2019, October 4). 10 companies that spent more than $1 billion in ads so you'd buy their products. Retrieved from https://www.businessinsider.com/10-biggest-advertising-spenders-in-the-us-2015-7

Federal Trade Commission. (2019, September 4). Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law. Retrieved from https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations

Fontana, F. (2018, March 29). Lawsuits Against Facebook Over Data Privacy Issues Are Piling Up. Retrieved from https://www.thestreet.com/technology/everyone-who-is-suing-facebook-for-cambridge-analytica-14536213

Funk, T. (2012). Facebook Advertising. In *Advanced Social Media Marketing: How to Lead, Launch, and Manage a Successful Social Media Program* (pp. 75–101). Apress L. P.

Golbeck, J., & Mauriello, M. L. (2016). User perception of Facebook app data access: A comparison of methods and privacy concerns. *Future Internet*, *8*(9). doi: 10.3390/fi8020009

González, E. M., & Vizcaíno-Laorga, R. (2018). Technophobic Dystopias: A Theoretical Approximation to the Communication Technology Limits Related to Privacy From the Google Glass Case and Audiovisual Fiction. *Journal of Information Policy*, *8*, 296–313. doi: 10.5325/jinfopoli.8.2018.0296

Henriquez, M. (2019, December 5). The Top 12 Data Breaches of 2019. Retrieved from https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019

Hoffower, H. (2020, January 29). 9 mind-blowing facts that show just how wealthy Facebook CEO Mark Zuckerberg really is. Retrieved from https://www.businessinsider.com/how-rich-is-mark-zuckerberg-net-worth-mind-blowing-facts-2019-5

Huang, Y., Hui, S., Inman, J. J., & Suher, J. (2013). The effect of in-store travel distance on unplanned purchase: Applications to mobile promotion strategies. *Journal of Marketing*, *77*(2), 1–16. doi: https://doi.org/10.1509/jm.11.0436

International Comparative Legal Guides. (2019, March 7). Data Protection Laws and Regulations. Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Janjigian, L. (2016, August 23). Facebook can guess your political preferences - here's how to see how it's categorized you. Retrieved from https://www.businessinsider.com/facebook-can-guess-your-political-preferences-2016-8

Johanssen, J. (2018). Gaming–playing on social media: Using the psychoanalytic concept of "playing" to theorize user labour on Facebook. *Information, Communication & Society*, *21*(9), 1204–1218. doi: 10.1080/1369118x.2018.1450433

Macaraeg, M. J. (2017). From atoms to bits: Personal data privacy and security in the information society. *Ateneo Law Journal*, *62*(1), 223–258.

Macrotrends. (n.d.). Facebook Net Worth 2009-2019. Retrieved April 25, 2020, from https://www.macrotrends.net/stocks/charts/FB/facebook/net-worth

Malgieri, G., & Custers, B. (2018). Pricing privacy – The right to know the value of your personal data. *Computer Law & Security Review*, *34*(2), 289–303. doi: 10.1016/j.clsr.2017.08.006

Matz, S. C., Menges, J. I., Stillwell, D. J., & Schwartz, H. A. (2019). Predicting individual-level income from Facebook profiles. *Plos One*, *14*(3). doi: https://doi.org/10.1371/journal.pone.0214369

Nyoni, P., & Velempini, M. (2018). Privacy and user awareness on Facebook. *South African Journal of Science*, *114*(5), 27–31. doi: 10.17159/sajs.2018/20170103

Pence, H. E. (2015). Will big data mean the end of privacy? *Journal of Educational Technology Systems*, *44*(2), 253–267. doi: 10.1177/0047239515617146

Perez, S., & Whittaker, Z. (2018, September 28). Everything you need to know about Facebook's data breach affecting 50M users. Retrieved from https://techcrunch.com/2018/09/28/everything-you-need-to-know-about-facebooks-data-breach-affecting-50m-users/

Pew Research Center. (2019, June 12). Mobile Fact Sheet. Retrieved from https://www.pewresearch.org/internet/fact-sheet/mobile/

Reyes, M. S. (2019, April 26). Scandals and teen dropoff weren't enough to stop Facebook's growth. Retrieved from https://www.businessinsider.com/facebook-grew-monthly-average-users-in-q1-2019-4

Rojas, N. (2018, June 5). The New Rules on Social Media, Privacy and Data Protection. Retrieved from https://topdogsocialmedia.com/privacy-and-data-protection/

Sobers, R. (2020, March 29). 107 Must-Know Data Breach Statistics for 2020. Retrieved from https://www.varonis.com/blog/data-breach-statistics/

Solon, O. (2018, April 19). How Europe's “breakthrough” privacy law takes on Facebook and Google. Retrieved from https://www.theguardian.com/technology/2018/apr/19/gdpr-facebook-google-amazon-data-privacy-regulation

Solove, D. J., & Schwartz, P. M. (2018). *Information Privacy Law* (6th ed.). New York: Wolters Kluwer Law & Business.

Spangler, T. (2019, November 22). YouTube Creators Worried and Confused Over New Kid-Video COPPA Rules, Potential Fines. Retrieved from https://variety.com/2019/digital/news/youtube-coppa-rules-children-videos-fines-1203413642/

Stewart, L. (2019). Big data discrimination: Maintaining protection of individual privacy without disincentivizing businesses' use of biometric data to enhance security. *Boston College Law Review*, *60*(1), 349–386.

Sweney, M. (2019, July 8). BA faces £183m fine over passenger data breach. Retrieved from https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways

Tschider, C. A. (2015). Experimenting with privacy: Driving efficiency through a state-informed federal data breach notification and data protection law. *Tulane Journal of Technology & Intellectual Property*, *18*, 45–81.

Waldman, A. E. (2016). Privacy, sharing, and trust: The Facebook study. *Case Western Reserve Law Review*, *67*(1), 193–233.

Williams, M., Nurse, J. R., & Creese, S. (2019). Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior*, *99*, 38–54. doi: 10.1016/j.chb.2019.04.026

Winder, D. (2019, August 20). Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019. Retrieved from https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#789602f9bd54

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society*, *16*(4), 479–500. doi: http://dx.doi.org/10.1080/1369118X.2013.777757

Zharova, A. K., & Elin, V. M. (2017). The use of big data: A Russian perspective of personal data security. *Computer Law & Security Review*, *33*(4), 482–501. doi: 10.1016/j.clsr.2017.03.025

Author Biography

Michael “Pearce” Blend was born in Dallas, Texas on December 14, 1997. He grew up in Dallas and attended Cistercian Preparatory School in Irving. Pearce’s interest in the data privacy subject matter stemmed from his involvement with data analysis in university classes and summer internships and from his parents, who are both lawyers. He will graduate from the University of Texas at Austin in May 2020 as a Polymathic Scholar in the College of Natural Science with a Bachelor of Science and Arts in Mathematics and a Bachelor of Arts in Economics, along with two certificates in Elements of Computing and Evidence and Inquiry. After graduation, Pearce plans to enter the workforce as a business analyst in Texas.