5-2020

What Consumers Don't Know They're Giving Away (Data and Privacy Concerns)

Bayleigh Reeves

What Consumers Don't Know They're Giving Away (Data and Privacy Concerns)

by

Bayleigh N. Reeves

Advisor: Rebecca Miles

An Honors Thesis in partial fulfillment of the requirements for the degree Bachelor of Science in Business Administration in Marketing & Management.

Sam M. Walton College of Business
University of Arkansas
Fayetteville, Arkansas

May 9, 2020

Introduction

The modern world leverages technology and information captured by it in ways the inventors of these technologies likely never imagined. Phones and other devices are gathering information about consumers in the background when they do not even realize it. Pew Research Center found that about 77% of Americans own a smartphone and 88% use the internet. This mass access to technology and information tracking raises many privacy concerns. Basic demographic information is being tracked as well as more in-depth information like shopping tendencies, financial information, and information about known associates. While most of this data is being used for marketing and other functional purposes, the question is raised if the information is truly secure and only in the hands of the companies that consumers give it to. With consumers readily giving out personal information and also biometric data (such as fingerprint and Face ID) freely to companies like Apple, it makes some consumers worry about how safely their information is being guarded. Consumers are also worried as artificial intelligence becomes mainstream with products like Google Home and Amazon Echo embedded into the average consumer's home. Some people may not realize the risks of data collection and the importance of regulation in mitigating those risks. This paper will paint a better picture of the issue and educate consumers so that they are informed when they go online and when they vote. Today, consumers are overwhelmed with legal disclosures and technical information on the subject and this paper will make the vast amount of knowledge digestible and easy to read.

A better understanding of the risks will hopefully convince consumers that the issue is important enough to get them to change their privacy settings and to vote for congressmen who want data privacy regulation. This paper does not serve to warn against targeted marketing and having personalized ads. Instead it warns consumers about not knowing the full range of uses of their data. Whether their data is being shared with third parties, used for ulterior purposes, or is not secure in databases, consumers need to know. With regulation, companies will be held more accountable and will have to treat consumer data with more care and put in more safety precautions to prevent theft or hacking.

Regulation may seem daunting or unnecessary, and with any new regulation there will be naysayers, but hopefully most will see the benefit and public good. For example, it was not until the 1950s that seat belts in automobiles started being included by the manufacturer. They were not even required to be installed until 1968. However, the mandated use of seatbelts for drivers was not enforced until each state made their own laws on the matter. In 1984, New York was the first state to make a seat belt law requiring drivers to use them. Over the following 11 years, almost all of the other states created seat belt laws of their own. This issue was initially met with indifference and drivers did not see a need to wear the belts. Over time, data has proven the effectiveness and lifesaving benefits that seat belts provide. Over half of people today that die from car crashes are people that did not have on their seat belts (CDC: Motor Vehicles Safety, 2011). Seat belts and other vehicle safety measures and regulations are the reason why driving is much safer today than it was over 40 years ago (The History of Seat Belts, 2019).

While some may not see the need for data privacy regulations today, they may see them in the years to come. Will the number of data breaches be lower with regulation? Will consumer information be more secure? These questions will only be answered with regulation. Hopefully, with regulation consumers will see evidence in the need for privacy regulations in the number of data breaches lowering and more transparency in data usage.

This report will examine the following topics: (1) the trust consumers have in the companies they give information to; (2) what information is being collected and what are companies doing with it; (3) what can happen when data is in the wrong hands; (4) companies attitudes towards data privacy; and (5) current regulation on consumer data privacy. The purpose of this thesis project is to collect information available on the subjects and to create a digestible summary for the everyday consumer to easily read and understand. The problem currently is there is so much information available, but it is spread all over the internet with no clear connections. This paper will connect the information to educate the consumer and show them the importance in protecting their data and voting for legislation to regulate privacy in corporate use of personal data.

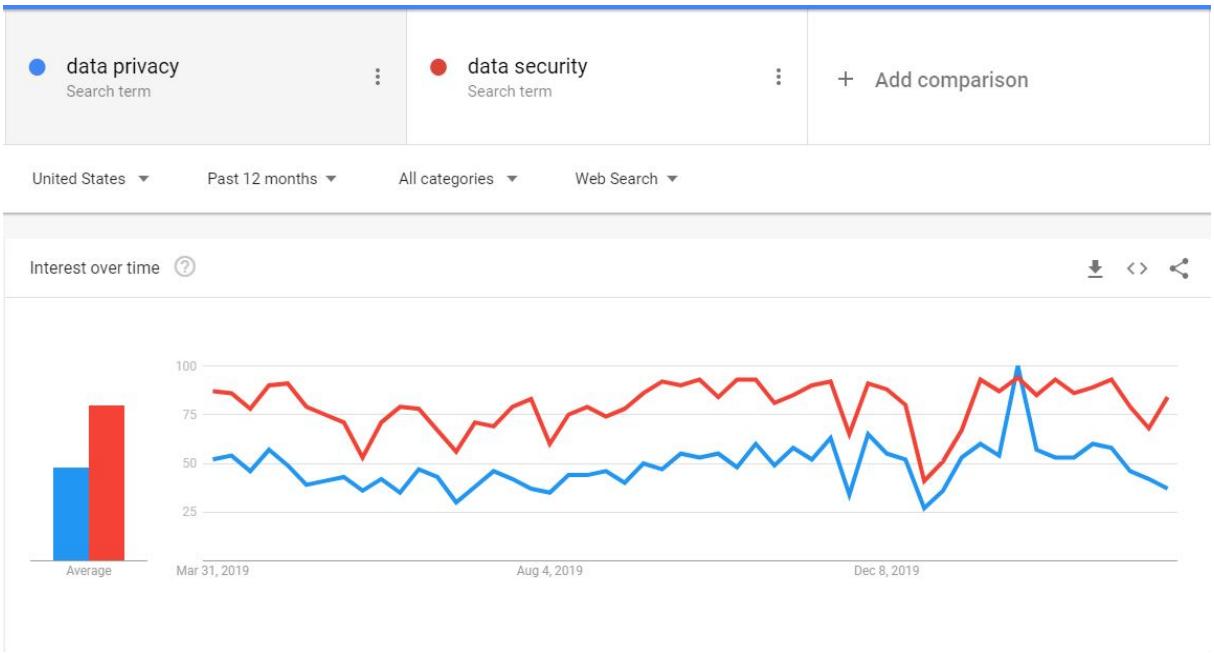
Deep Dive

Current attitudes towards data privacy and trust of technology range with different levels of education on the subject, but it is a growing consumer concern in a general sense. This literature review will discuss research completed to consolidate the information for consumers. The literature review consists of information collected from online databases and news articles. The paper discusses five different aspects of data privacy and how personal information is used for marketing and other purposes.

1. Do consumers trust the companies they give information to?

Consumer trust is a key part of a company's reputation. If consumers distrust a company for one reason or another, they might stop giving business to that company. As privacy concerns are on the rise, companies need to keep consumer trust as a top priority. Convenience is a top consumer priority, but data privacy tops the list as well. Consumers are especially concerned about giving control of their data to companies.

This concern for privacy is evident in the measure of Google searches for "data privacy" and "data security." In the chart below, the interest of the two terms being searched on the search engine is compared through Google Trends. The numbers on the chart represent search interest relative to the highest point on the chart for the given region (the United States) and time (the past 12 months which at the time of this paper is March 2019 to March 2020). A value of 100 is the peak popularity for the term. A value of 50 means that the term is half as popular. A score of 0 means there was not enough data for this term. The blue is the trend of popularity of the keyword "data privacy" and the red is the popularity trend of the keyword "data security." Overall, the search for "data security" is more popular over this period of time. This is most likely due to reactionary consumer searches of people wanting to protect their data rather than figuring out how their data is being used. However, data privacy spiked at the end of January 2020 with peak popularity around January 26th - February 1st (Google Trends, 2020). This was most likely due to "Data Privacy Day" that is held every year on January 28th. The purpose of the day is to raise awareness and to give consumers information on how to protect their data. Many companies observed the day in 2020 by publishing ways for consumers to protect information on their sites.



The concept of data privacy is still vague to consumers. They know they do not want their personal information shared without their direct input, but do not know how to protect their information and are unaware of the digital footprint they leave when browsing. The California Consumer Privacy Act and the General Data Protection Regulation are attempting to provide consumers with a more straightforward way of knowing if their data will be shared when using a website (Data Not for Sale, 2019). Regulations like these will be discussed in depth later in this report.

Consumers are introducing technology into their homes and everyday functions. Artificial intelligence (AI) devices such as Amazon Alexa or Google Home bring constant monitoring inside consumers' homes, listening constantly and waiting to be utilized. Only 38% of adults say that artificial intelligence is a useful addition to devices. This low percentage could be due to a lack of understanding of the technology or a general distrust. Less than one quarter of adults say they trust artificial intelligence. A study titled *Attitudes Toward Technology and the Digital World - US, November 2017* revealed that while most people trust AI to do small tasks like setting alarms or checking the weather, few people trust AI technology to do complex tasks such as managing a financial portfolio (Digital Trends, 2018).

In addition to concerns with Artificial Intelligence, facial recognition technology has continually raised the concerns of consumers due to the lack of information and regulation on how the data can be used. While privacy is the main concern, some opponents caution that the increased surveillance could lead to more discrimination and harassment from misidentification. The technology is also very discreet and does not require direct consumer interaction, making consent for the technology unclear (Faceless Concerts, 2019).

Another controversial data privacy topic with much consumer debate is personalization in advertising. Much of consumer research has shown that consumers feel uncomfortable and reject it. However, it can also be seen as more relevant and useful, creating a paradox where consumers have privacy concerns while also enjoying the benefits.

The table below has a summary of consumer research on perceptions of personalized advertising. In the table, the privacy concern is repeated time and time again, while the redeeming quality of relevance and user experience champion the practice of personalization.

Overview of Research on Consumer Perceptions of Personalized Advertising
*From most recent to most dated

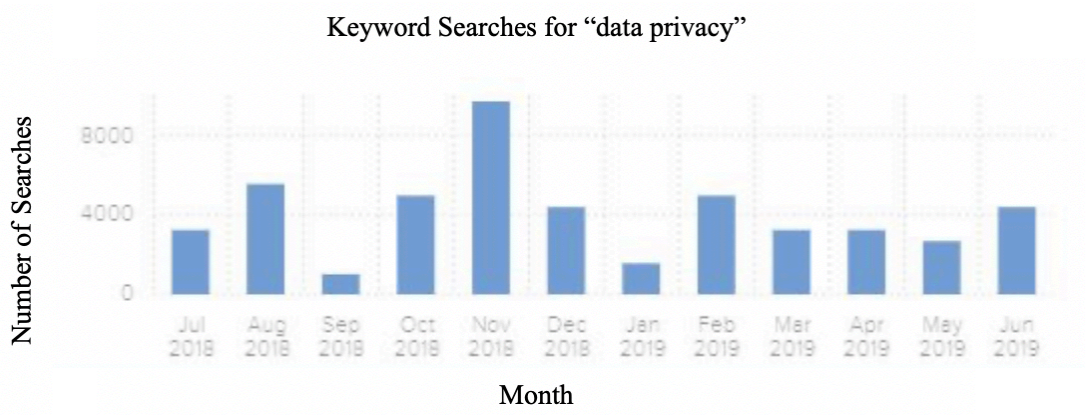
Authors	Main Findings & Arguments
Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . .de Vreese, C. H. (2018)	- decreases trust and anticipated benefits of personalization
Gironda & Korgaonkar (2018)	- the more useful a personalized advertisement is, increases its effectiveness - the degree of invasiveness of a personalized advertisement decreases its effectiveness.
Kim & Huh (2017)	- personalized advertisements are not experienced as more relevant. - the concern for privacy lowers consumer trust towards personalized advertisements. - the relevance of a personalized advertisement to a consumer improves consumer attitude towards it
Bang & Wojdynski (2016)	- consumers notice personalized ads over generic ads.
Bleier & Eisenbeiss (2015)	- personalized advertising improves utility of ads for trusted retailers. - personalization for less trusted retailers can increase backlash and privacy concerns - click-through intention is influenced by ad relevance, reactance and privacy concern
Tucker (2014)	- perceived control over privacy increases effectiveness of personalized advertising.
Kim & Han (2014)	- personalization increases explanation, credibility, and entertainment of advertising. - personalization lowers ad annoyance.
Baek & Morimoto (2012)	- privacy concern and ad annoyance increase skepticism and avoidance for personalized advertising. - personalization decreases ad skepticism and ad avoidance.
Goldfarb & Tucker (2011)	- personalization of advertising combined with advertising prominence lowers effectiveness of the ad for consumers concerned about their privacy.

Infogroup recently surveyed over 1,500 consumers to see current attitudes about personalized advertising. In the survey, 93% of respondents said they receive marketing communications not relevant to them. In a follow-up question, 44% said they are willing to switch to brands that have more personalized communications. A majority of 90% said they find irrelevant advertisements annoying. Millennials ranked personalization as being most critical to earning and keeping their business. Respondents cited the following requirements to ensure relevant communications: relevant to my interests, product details, is a product or brand I already enjoy, tells a good story, and makes me laugh. When asked what their pet peeves with brand communications were, they said: talking about topics I have no interest in, trying to sell me things I already own, misspelling my name, getting my identity or gender wrong, and getting my location wrong. This survey points out that consumers do not mind and even prefer personalization when used correctly (Zawacki, 2019).

While many companies use the data for personalized ads of their own, some companies give or sell the data to third parties. A survey from Britepool and Annenberg Research states that 87% of participants would select an opt-out option for selling their personal information to third parties. In the same study, respondents were asked if they would exchange personal information for rewards. The percentage of respondents that would opt-out dropped to 61% and 21% of respondents said they would choose rewards (Data Not for Sale, 2019).

Not only are consumers worried about their data privacy, they are also very curious about it. In the graph below from Wordtracker, the number of keyword searches for “data privacy”

from July 2018 to June 2019 fluctuated from around 1000 to over 8000 searches per month with the average being about 4,074 searches per month (Wordtracker, 2020). The spike in the number of searches in November of 2018 is due to the Facebook privacy scandal. The New York Times published an exposé in November of 2018 with over 50 interviews of former Facebook employees revealing massive coverups and data privacy concerns the company ignored.



With consumer trust being an ongoing concern for companies, they must navigate the data privacy argument and their own positions. They must first assess what they are currently doing and what others are doing with data. Then, they can form their own policies and regulations to ensure consumers are being heard and protected.

2. What information is being collected and what are companies doing with it?

There are countless examples of companies using new technology in a way to enhance their overall interface, experience, or efficiency. Some of these new technologies, or new ways of applying capabilities, utilize consumer information in ways that have never been attempted (or publicized) before now.

In 2018, Ticketmaster, an entertainment company specializing in ticket sales and event management, announced they would use facial recognition technology at events instead of ticket scanning to increase speed and convenience (Mintel). That same year, a similar technology was used, without consumer consent, at a Taylor Swift concert to detect known stalkers of the singer. Although the Taylor Swift concert security measures were arguably unethical, they were not illegal which shows the need for regulation and legislation on facial recognition technology (Stalker-Free Concert, 2018). Facial recognition technology is spreading into other areas besides event security. It has been applied to commercial convenience, home security, business security, and personal technology security (iPhone Face ID). Even though consumers are voicing concerns about their personal information being tracked through face and voice technology, they are still handing it over for convenience and access to popular services (Stalker-Free Concert, 2018).

Many companies use the personal data for personalization and convenience purposes as consumers are often shown digital advertisements based on their data (Data Not for Sale, 2019). The definition of personalization in online advertising is, "the strategic creation, modification,

and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors" (Strycharz, 2019). Their characteristics are tracked through cookies and advertisements are served through targeting and retargeting. Retargeting and cookies track what consumers look at online in an attempt to serve individual consumers advertisements for products they might be interested in based on their personal online activity. The personalization can be seen in a number of ways. The ads can address consumers by name, or the data can be configured more complexly by personalizing content or distribution.

Personalization has been viewed as an effective and efficient way to communicate with customers. It provides the consumer with a relevant advertisement and might lead to a purchase they feel happy about. Today, most successful digital advertising campaigns require some form of personalization or targeting to reach their target consumers. It is almost seen as a waste of money to have a digital advertisement without targeting or personalization technology (Zawacki, 2019).

Some companies, however, have been caught using information for ulterior purposes. In 2014, it was revealed that ride-hailing company Uber had been able to track customers and that employees were misusing this information to track high-profile celebrities, ex-partners, and politicians. This tracking occurred in real-time without consent of the customers. The FTC accused Uber of not limiting the use of customer data by employees, when it could have been prevented by several low-cost measures. The company is now subject to third-party audits of its privacy practices for the next 20 years.

Another example of data misuse is in law enforcement. Both the state of Minnesota's police department and Chicago Police Department have been accused of misuse of data. Many employees have been found to be searching criminal and civil databases as well as driver information databases for people that are not involved in any police business or investigations. For example, one Minnesota woman reported her ex-fiancé wrongfully searched for information on her and her family over 100 times after they broke up (The Associated Press, 2016).

In 2015, AT&T paid a $25 million fine to the FCC for multiple data breaches that leaked as many as 279,000 customer's records, including names, phone numbers and even Social Security numbers. Outside companies paid AT&T call center employees to provide sensitive customer information. The breaches happened in foreign call centers in Mexico, Colombia, and the Philippines. The information accessed is protected by federal regulations. In the wrong hands, the information can be used to obtain "unlock" codes so that mobile phones can be used with any wireless carrier. Stolen phones that are unlocked are worth more on the black market because they can be sold anywhere. The FCC stated that the Mexico breach lasted longer than five months between 2013 and 2014 and that three contractors accessed 68,000 customer records to request more than 290,000 unlock codes illegally from AT&T. AT&T responded by changing policies and strengthening operations to prevent further incidents. The settlement covered free credit monitoring for those affected (Fung, 2015).

A major breach of financial information came in 2015 when Morgan Stanley discovered that one of its financial advisors accessed data on around 10% of the company's clients (about 350,000 people) and publicly posted details about 900 clients online. The information was posted on an anonymous text sharing site, Pastebin. Morgan Stanley found and removed the information with little damage done (Chickowski, 2015). While the incident caused little damage, the fact that a mid-level employee was able to access and post so much customer information easily is

unsettling. The incident should serve as a warning to companies to prevent similar, and possibly worse, situations from happening.

Data is constantly being collected and passed from company to company for a multitude of purposes. Some companies are clear on what they are doing with the data while others are vague or secretive. Other companies make glaring oversights that cause massive scandals and breaches of privacy. With data privacy scandals and misuse happening very frequently today, consumers are left to wonder: "Who is protecting my data?"

3. What can happen when data is in the wrong hands: The Facebook/Cambridge Analytica scandal

The Facebook and Cambridge Analytica Privacy scandal is a recent example of data misuse. In 2018, when the news of the Facebook/Cambridge Analytica scandal broke, it caused widespread confusion and fear among Facebook users and the public. Cambridge Analytica once promised to "find your voters and move them to action" but ended up filing for bankruptcy in May 2018 due to media coverage that drove away the company's customers amid the scandal it was involved in with Facebook. It all started in March 2018 when a whistle-blower came forward, an ex-employee of Cambridge Analytica, Christopher Wylie, and leaked the scandal to the *Observer*. The whistleblower claimed that Cambridge Analytica used Facebook to gain access to millions of profiles and used this data to target voters with personalized political advertisements. (What can we learn from the Facebook–Cambridge Analytica scandal?, 2018).

The data apparently came from an app created in 2013 by Aleksandr Kogan. Back in 2013, Facebook allowed app developers to collect data about app users as well as their Facebook friends. In a written evidence statement, Kogan confirmed the app collected data from Facebook friends of the users if the privacy settings were not changed, allowing access to friends' information including name, birthday, location, and gender. The data accessed could be personally linked to over 87 million people (Sanders & Patterson, 2019).

Cambridge Analytica was the most publicized, but not the only company involved. These companies gained access due to a variety of factors including lack of safeguards against data harvesting, a lack of monitoring developers by Facebook, and users agreeing to extremely broad terms & conditions. Cambridge Analytica was able to harvest data through a personality quiz based on the OCEAN model (OCEAN stands for openness, conscientiousness, extraversion, agreeableness, and neuroticism). This allowed the company to create a psychographic profile of users. Adding the app to a Facebook account to take the quiz allowed the app creators access to profile information and user history, as well as their Facebook friends' profile information and user history. This data included user and friends' Facebook likes (Sanders & Patterson, 2019). The information gained through this quiz could be used to "automatically and accurately" predict highly personal sensitive information and attributes such as: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender using a model developed by the company (Sanders & Patterson, 2019).

While news of this scandal did not break until 2018, the scandal can be tracked all the way back to 2014 when Kogan requested that people add the app to their Facebook account with the alleged wording, "provide our app access to your Facebook so we can download some of your data--some demographic data, your likes, your friends list, whether your friends know one another, and some of your private messages." In 2015, Facebook learned that the data Kogan

collected through the app was shared with Cambridge Analytica. Facebook's Mark Zuckerberg claims, "we immediately banned Kogan's app from our platform, and demanded that Kogan and Cambridge Analytica formally certify that they had deleted all improperly acquired data. They provided these certifications." In 2016, Cambridge Analytica took legal action against Kogan for giving them "illegally acquired data," (Sanders & Patterson, 2019).

In March of 2018 the whistleblower article was published by The Guardian and The New York Times. Later that month, the FTC opened an investigation for Facebook and in May the FBI and Justice Department were opening an investigation on Cambridge Analytica. On May 16, 2018, Christopher Wylie testified before the Senate and said that Cambridge Analytica, under the instruction of Steve Bannon, meant to "exploit certain vulnerabilities in certain segments to send them information that will remove them from the public forum, and feed them conspiracies and they will never see mainstream media." He also revealed that the company targeted people that according to the model would vote for the Democratic party, especially African American voters. Russian interference in the elections was evident (Sanders & Patterson, 2019).

In June of 2018, an article in the New York Times reported Facebook maintained data-sharing partnerships with device manufacturers including Apple, Amazon, BlackBerry, Microsoft, and Samsung. While Facebook claimed this was solely for the purpose of offering "the Facebook experience" on the devices, the article indicated the access also allowed manufacturers to access data on a Facebook user's friends, even if the friends had privacy settings blocking data sharing with third parties. Several days after this article was published, it was revealed that Chinese device manufacturers Huawei, Lenovo, Oppo, and TCL also had similar partnerships with Facebook. This caused the US government to become worried that these partnerships posed national security risks. In July, the UK fined Facebook £500,000 for its role in the data scandal. In late 2018, before the midterm elections, Facebook continued to crack down on false accounts and political advertising, requiring political advertisements to have identity verification when paying. They also banned false information about voting in the midterm election (Sanders & Patterson, 2019).

In November 2018, The New York Times published its exposé which revealed even more layers of the scandal including:

- In early 2016, a Facebook security expert told Chief Security Officer Alex Stomos that Russian hackers were combing through accounts for people connected to the presidential campaigns, which Stamos then told general counsel Colin Stretch
- A group named "Project P" was formed by Zuckerberg (founder and CEO) and Sandberg (COO) to observe false news on the site. By January 2017, the group wanted to publish a paper to the public about their findings, but was stopped by board members and Facebook VP of Global Public Policy Joel Kaplan (who had worked in former President George W. Bush's administration)
- In 2017, Facebook was claiming publicly that there was no Russian effort of any significance on Facebook, despite ongoing internal investigation into the Russian involvement

In late November 2018, it was discovered that a company called Six4Three developed an app that used image recognition to identify photos of bikini-clad women on Facebook users' friends' pages. The company had to hand over documents about Facebook to Parliament. These documents revealed that Facebook entered into agreements with Lyft, Airbnb, Bumble, Netflix, and other companies that allowed these groups full access to friends' data after this type of

agreement was discontinued by Facebook. The documents also revealed that Facebook used data collected through a VPN service to survey the use of mobile apps on smartphones in order to determine what companies to acquire and which were threats (Sanders & Patterson, 2019).

In December of 2018, The New York Times reported that Facebook had special agreements with companies such as Bing, Netflix, Spotify, Amazon, and Yahoo that allowed them access to data such as friend lists and private messages. Facebook had previously stated they stopped agreements such as this type of data sharing years earlier. Facebook claimed the data was about "helping people" and it was done with user consent (Sanders & Patterson, 2019).

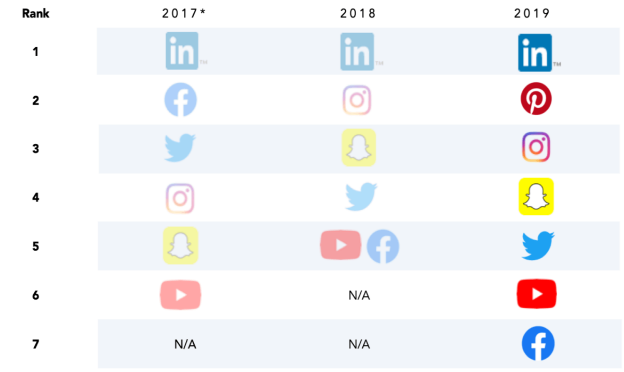
In March 2019 Zuckerberg announced plans to rebuild encryption and privacy services over the next few years. Privacy settings have been adjusted and are more customizable to the user now. Zuckerberg also published an op-ed in the Washington post calling for governments to take an active role in regulating the internet. In July 2019, Facebook settled with the FTC for $5 billion over the privacy violations. Facebook agreed to conduct an overhaul of current consumer privacy practices and access to friend data was immediately restricted. Separate settlements with Aleksandr Kogan and Cambridge Analytica's former CEO restricted how they could conduct future business and required them to delete any personal information collected (Sanders & Patterson, 2019).

The seemingly unbelievable events of the Facebook Cambridge Analytica data privacy scandal highlight the need for regulation and legislation on data privacy and how companies can use personal consumer data. Victims of this privacy scandal had their personal information shared as well as the personal information of their friends (who had no part in consent or negligence). Not only were psychographic profiles made for the affected users, but some Facebook users even had private messages on Facebook being accessed by companies.

The chart below from Business Insider shows the ranking of trust for top social media sites for 2017, 2018, and 2019. In 2018, the overall ranking was changed to be calculated as the average of pillar ranks (security, legitimacy, user experience, shareability, and relevance). LinkedIn came in as the most trusted in all three years. However, Facebook started as second place in 2017 and dropped to the least trusted of the seven in 2019. In 2018 Facebook tied for last with YouTube. These digital trust rankings for Facebook most likely fell because of the Cambridge Analytica scandal that continues to unfold (Digital Information World, 2019).

Business Insider Intelligence's 2019 Digital Trust Ranking

Ranking based on overall Digital Trust scores



**Ranking methodology changed for 2018 onward.*
Note: Our overall ranking is calculated as an average of pillar ranks. Pillars are: Security, Legitimacy, Community, User Experience, Shareability, and Relevance.
Source: Business Insider Intelligence Digital Trust Report 2017, 2018, 2019

PRIMARY RESEARCH FROM BUSINESS INSIDER INTELLIGENCE

4. How do companies feel about consumers' data privacy and what are they doing to protect it?

The concept of data privacy creates a tension between corporate profit and the public good. One big reason companies track consumer data is to serve them personalized advertisements that the consumer will click through and purchase the product. Giving up this tactic would possibly decrease profits and make advertising less strategic and profitable. However, with rising consumer concern and regulations being put in place in some parts of the world, companies are responding in numerous ways.

Many companies that do business in California or the European Union have already adjusted their privacy policies for other regions that are not covered under the California Consumer Privacy Act (CCPA) or the European Union's General Data Protection Regulation (GDPR). Implementing consent in areas outside of these regions makes it easier for the companies to roll out consent in all markets rather than making it by region. If legislation were passed in the United States, many bigger companies will not have to change too much about their privacy policy.

In recent news, Apple released an update to its Safari web browser's Intelligent Tracking Prevention (ITP), a feature that allows it to block cookies and prevent advertisers from seeing web activity. Safari now blocks all third-party cookies. This means that by default, no advertiser or website can follow a consumer's web activity using the tracking technology. With this significant improvement in technology, they have come out ahead of Google who said they would have third-party tracking technology phased out by 2022 (Statt, 2020). Apple is a great example of a tech company, who has been previously criticized for privacy concerns (biometric data, etc.) releasing technology that protects consumer data rather than releasing a platform that encourages more tracking.

Many companies are adjusting their privacy policies, but is it enough? What will it take for everyone's data to be more secure once and for all? After the CCPA and GDPR were passed, companies reacted. Many adjusted policies worldwide, but there are still so many companies whose policies still have not changed, and their users' data is still unsafe. Legislation and regulation are the only ways that consumers' data will be protected.

5. What regulation currently exists for protecting consumer privacy?

As data privacy becomes a bigger conversation, regulation and legislation is being discussed and implemented in many areas globally. This push around consumers accessing more knowledge about how their information is being used is groundbreaking and legislators and governments are finally starting to listen and respond. Consumers controlling what is done with their information and that information remains secure are the top priorities. Passing legislation on data privacy will create consumer security and trust.

The California Consumer Privacy Act, passed in 2018 required websites to educate visitors on how their data will be used and shared with third parties and must include an opt-out button option which explicitly states messaging along the lines of "Do Not Sell My Personal Information" (Data Not for Sale, 2019). The CCPA went into effect on January 1, 2020 and applies to around 500,000 companies doing business with residents of California, even if they are not physically located there. Companies must carefully handle data such as name, address, location, SSN, financial information, and more. Users have the right to know what information

will be collected, the right to request deletion of their data, and the right to opt out of services and prevent the sale of their information. If companies do not comply, they are subject to a fine of up to $7,500 per violation and potential class-action lawsuits (Jalil, 2019). The CCPA follows similar guidelines of the General Data Protection Regulation (GDPR) from the European Union.

The European Union's General Data Protection Regulation (GDPR), which went into effect in May 2018, strictly regulates retargeting and the use of cookies (Innovate or Hunker Down, 2019). This legislation not only affects businesses in the European Union, but any company outside of the European Union that offers goods or services to customers or businesses there. It serves to ensure companies inform users on how their information is used and gives them the right to opt out (Jalil, 2019).

In September 2019, a group of 51 CEOs from the Business Roundtable advocacy group sent a letter to Congress asking them to pass a "comprehensive consumer data privacy law." Companies involved include Amazon, AT&T, IBM, Motorola, and Qualcomm. They say that state laws on privacy vary too much which leads to confusion for customers. A federal law would create trust and a "stable policy environment" that allows companies to operate within one set of boundaries rather than the varied boundaries the states pose. They published a framework for their ideas highlighting that a consumer privacy law should: "champion consumer privacy and promote accountability, foster innovation and competitiveness, harmonize regulations, and achieve global interoperability." This not only would protect consumers but ensure that companies do not get in trouble for data practices (Fingas, 2019).

In March 2020, Senator Jerry Moran introduced the Consumer Data Privacy and Security Act of 2020 (the CDPSA). The CDPSA aims to create an overarching federal framework for consumer data privacy. It has integrated topics and regulations from both the California Consumer Privacy Act and the European Union's General Data Protection Regulation to provide a more holistic solution (Kratofil, 2020). Some specifics of the act, if passed, are that it will:

- Exempt "small businesses" (those with less than 500 employees) from some parts of compliance
- Overrule most state and local laws on data privacy
- Overrule most previous federal laws on data privacy except for: The Children's Online Privacy Protection Act ("COPPA"), Communications Assistance for Law Enforcement Act, Section 227 of the Communications Act of 1934, Title V of the Gramm-Leach-Bliley Act ("GLBA"), The Fair Credit Reporting Act, The Health Insurance Portability and Accountability Act ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), The Family Educational Rights and Privacy Act ("FERPA"), Electronic Communications Privacy Act, The Driver's Privacy Protection Act of 1994, and the Federal Aviation Act of 1958.
- Designate the FTC as the agency in charge of administering the CDSPA.
- Establish two forms of consent
    - 1. Implicit consent: an individual has given consent to collection or processing of personal data if they did not decline the request after being given notice and a reasonable amount of time has passed
    - 2. Express affirmative consent: when collection or processing involves sensitive personal data or third-party use of data. To be valid, this type of consent must be: (1) clearly, prominently, and unmistakably stated, (2) in

response to a request to collect or process personal data, and (3) cannot be assumed from no action

- Establish a "Permissible Purposes" for data collection without consent to include when it is being used:
    - To provide a service or perform a contract
    - To comply with laws
    - To prevent danger to the personal safety of any individual
    - To prevent fraud and protect security of the company's, service providers', or individual's rights, property, services, or information systems
    - For research performed by the company or service provider (at the direction of the company)
    - For the company's or service provider's operational purposes. Operation purposes include internal operations (e.g., billing, website maintenance, financial reporting); temporary storage; marketing or advertising; to improve products and services; and any additional specific purposes defined by the FTC.
- Require companies to have their new privacy policies in an accessible place, written in an "easy-to-understand" way. Companies also must publish previous versions of their privacy policies. A third requirement is companies must provide notice of any changes in their privacy policies
- Provide two ways a company may collect or process data.
    - 1. With consent from the individual
    - 2. If the collection is done for a "Permissible Purpose"
- Provide ways a third-party company may collect or process data
    - 1. If the original company discloses the third party will be collecting the personal data and the consumer consents
    - 2. the collection or processing by the third party is done for the limited permissible purpose

(Kratofil, 2020).

While it is unclear which, if any, proposed data privacy legislation will be put before Congress, the Consumer Data Privacy and Security Act seems promising. It takes into consideration key data privacy trends seen in legislation like the California Consumer Privacy Act and the European Union's General Data Protection Regulation. It establishes vast privacy rights for consumers and strict penalties for violations of the act, if passed (Kratofil, 2020). With other countries and government entities like the European Union and California passing and enforcing legislation protecting consumers online, it is time for the United States to pass a federal framework of data privacy laws and regulations. Data privacy is a hot topic right now and the United States needs to take action before more data privacy scandals occur.

Implications for Consumers: "So What?"

This project explores several of the layers that make up data privacy and regulation. But for what purpose? It aims to warn and educate consumers of all ages about the dangers of unprotected data. Implications and warnings have been broken down by three key age groups: young adults (18-30), adults (31-64), and seniors (65 and up). The reason they are broken up this

way is because these three groups grew up with varying levels of technology and therefore have different levels of understanding and expertise when it comes to technology and data privacy.

The first group, young adults aged 18-31, have grown up with technology in every aspect of their lives. The Internet has been around most, if not all, of their lives. Many are familiar with data privacy issues such as the Facebook/Cambridge Analytica scandal even if they do not understand it completely. This being said, they also tend to trust online services because it's what they have known growing up (Alton, 2017). The young adults have the biggest potential to change data privacy regulation, they are the generation that has most recently entered the voting population and can make a difference in the way they vote and protect themselves online. They must first be educated fully on how to protect themselves (through changing privacy settings and reading what their information is being used for on different websites). It is also up to this younger generation to educate some of the older generations to protect them and help them navigate confusing technology and privacy issues.

The second group, adults aged 31-64, are less trusting of technology because a majority of them remember when the Internet started and when social media and the age of the Internet took over. It is in this group's best interest to educate themselves on data privacy so that their personal and financial information is safe as they prepare for retirement. It is also this group's responsibility to educate their children and grandchildren on data privacy as they raise them in a world surrounded by technology that has so much information about them already. If this group can educate the newest generation, the new generation will value data privacy and make a change as well. Above all, adults can vote for legislators that support data privacy regulation.

The third group, seniors aged 65 and older, are at the highest risk for data breaches. As the highest risk group, they need to take several precautions including: creating strong passwords, downloading security software, adjusting browser settings, recognizing scam emails, and asking for help from family members or professionals on data security. These measures can protect them from further breaches and ensure peace of mind for a generation that is not so trusting of technology. All age groups should take these precautions in protecting their data, but seniors are the least likely to do so already. As the senior population has high voter turnout, they have a strong power to change legislation by electing people who care about data privacy and wish to pass legislation on the regulation of personal data usage. Even though seniors may not be the most technology savvy, they can ask for help from family members or professionals in order to stay safe online and prevent financial and personal data from ending up in the wrong hands.

Different generations must protect themselves in different ways as they have different experiences and use for technology. Data breaches and hackers do not discriminate by age. Every age group that I discussed has the ability to protect themselves and others from data privacy issues and breaches. Also, all of them can vote to make sure that the right people are in office to create change and pass legislation on data privacy regulation so that the United States population as a whole can be more secure online.

Conclusion

With the conclusion of this thesis project, I hope to have informed the everyday consumer about data privacy in an easy to read format that allows them to better understand the issues and current regulations. It is my intention to grant the consumer a better look at current legislation around the world and proposed legislation for the United States. Data privacy is a multi-faceted and complex topic that can be difficult to understand.

Data privacy laws will soon be similar to seat belt laws, consumers do not know they need it until they see the data behind regulation. In the beginning, many did not see the need behind the seat belt laws and saw seat belts as an unnecessary precaution. The facts convinced them later, years after the implementation of laws when they saw the statistics behind the life-saving seat belts. Initially when seat belt laws were enforced, drivers didn't see immediate benefit because of the increased number of drivers on the road. Pedestrian and passenger deaths offset the driver lives saved at first. The Peltzman effect theorizes that the perceived safety of seat belts and other safety features caused more people to drive and allowed them to drive more aggressively believing they were safe (Peltzman, 1975).

Hopefully, data privacy legislation and regulation will not be affected by a similar Peltzman effect where people believe they are safe online after regulation and not take additional steps to protect themselves. If they continue to take precautions after regulation, they will see the lowered amount of data breaches and identity theft. In 2018, there were 1.244 billion data breaches in the U.S. alone, which exposed over 446 million records (Statistica, 2019). Exposed records can lead to identity theft which is a major problem online today. Every 2 seconds there is a victim of identity theft and in America, nearly 60 million people have been a victim (Cooper, 2019). Data privacy affects billions. There are over 4 billion people in the world who have access to the Internet. The European Union has stepped up to try to solve data privacy issues in its own region. If the United States took a stance on data privacy by passing legislation and regulating the use of personal data, it could cause companies doing business in the U.S. bound by the legislation to enact data privacy precautions in other markets. Hopefully, this would create a ripple effect that would cause other countries to follow suit with data privacy legislation. If countries banded together to regulate data privacy globally, it would save millions, maybe even billions, of people from being victims of insecure data and possible identity theft.

Will data privacy legislation of the 2020's be the new seat belt laws of the 1980s? American consumers have the power to put pressure on their congressmen to push forward data privacy laws. Consumers can vote for representatives and senators that have data privacy legislation as part of their platform. Data privacy is everyone's responsibility. It may fall on the companies to protect the data, but consumers need to speak up and let legislators know of their concerns in data privacy and the need to pass a general data privacy framework for the United States.

References

5 Examples of Data & Information Misuse. (2019, October 22). Retrieved from https://www.observeit.com/blog/importance-data-misuse-prevention-and-detection/

Ali, A. (2019, September 29). Survey: LinkedIn, Pinterest and Instagram are the most trusted social media platforms. Retrieved from https://www.digitalinformationworld.com/2019/09/which-social-media-platform-do-you-trust-the-most.html#

Alton, Larry. "How Millennials Think Differently About Online Security." Forbes, Forbes Magazine, 1 Dec. 2017, www.forbes.com/sites/larryalton/2017/12/01/how-millennials-think-differently-about-online-security/#593b2f97705f.

Baek, T. H., & Morimoto, M. (2012). Stay away from me: Examining the determinants of consumer avoidance of personalized advertising. Journal of Advertising, 41(1), 59–76. https://doi.org/10.2753/JOA0091-3367410105

Bang, H., & Wojdynski, B. W. (2016). Tracking users' visual attention and responses to personalized advertising based on task cognitive demand. Computers in Human Behavior, 55, 867-876. https://doi.org/10.1016/j.chb.2015.10.025

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. Journal of Retailing, 91, 390-409. https://doi.org/10.1016/j.jretai.2015.04.001

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., . . .de Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. Journal of Computer-Mediated Communication, 23, 370-388. https://doi.org/10.1093/jcmc/zmy020

Chickowski, E. (2015, January 6). Morgan Stanley Insider Case Offers New Year Insider Reminders. Retrieved from https://www.darkreading.com/attacks-breaches/morgan-stanley-insider-case-offers-new-year-insider-reminders/d/d-id/1318501

Clement, J. (2020, March 10). U.S. data breaches and exposed records 2019. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Cooper, T. (2020, January 6). 26 Crucial Data Privacy Statistics (Updated Nov 2019). Retrieved from https://broadbandnow.com/report/26-data-privacy-statistics-2019/

Federal Privacy Legislation Update: Consumer Data Privacy and Security Act of 2020. (2020, March 14). Retrieved from https://www.natlawreview.com/article/federal-privacy-legislation-update-consumer-data-privacy-and-security-act-2020

Ferrell, O. C. (2017). Broadening marketing's contribution to data privacy. Journal of the Academy of Marketing Science, 45(2), 160-163. doi:http://dx.doi.org/10.1007/s11747-016-0502-9

Fingas, J. (2020, February 18). 51 companies tell Congress it's time to tackle data privacy. Retrieved from https://www.engadget.com/2019-09-10-tech-companies-ask-congress-for-data-privacy-law.html

Frenkel, S., Confessore, N., Kang, C., Rosenberg, M., & Nicas, J. (2018, November 14). Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis. Retrieved from https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html

Fung, B. (2015, April 8). AT&T will pay $25 million after call-center workers sold customer data. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/04/08/att-will-pay-25-million-after-call-center-workers-sold-customer-data/

Gironda, J. T., & Korgaonkar, P. K. (2018). iSpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. Electronic Commerce Research and Applications, 29, 64-77. https://doi.org/10.1016/j.elerap.2018.03.007

Goldfarb, A., & Tucker, C. (2011). Online display advertising: Targeting and obtrusiveness. Marketing Science, 30, 389-404. https://doi.org/10.1287/mksc.1100.0583

Google Trends: Data Privacy vs. Data Security. (n.d.). Retrieved from https://trends.google.com/trends/explore?geo=US&q=data privacy,data security

Jalil, R. (2019, December 30). Council Post: How Companies Are Preparing For The Shifting Data Privacy Landscape. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2019/12/30/how-companies-are-preparing-for-the-shifting-data-privacy-landscape/#14643c5d1599

Kim, H., & Huh, J. (2017). Perceived relevance and privacy concern regarding online behavioral advertising (OBA) and their role in consumer responses. Journal of Current Issues & Research in Advertising, 38, 92-105. https://doi.org/10.1080/10641734.2016.1233157

Kim, Y. J., & Han, J. (2014). Why smartphone advertising attracts customers: A model of Web advertising, flow, and personalization. Computers in Human Behavior, 33, 256-269. https://doi.org/10.1016/j.chb.2014.01.015

Morgan, R. (2017, August 16). Uber settles federal probe over 'God View' spy software. Retrieved from https://nypost.com/2017/08/15/uber-settles-federal-probe-over-god-view-spy-software/

Peltzman, S. (1975). The Effects of Automobile Safety Regulation. Journal of Political Economy, 83(4), 677-725. Retrieved April 29, 2020, from www.jstor.org/stable/1830396

"Policy Impact: Seat Belts." Centers for Disease Control and Prevention, Centers for Disease Control and Prevention, 3 Jan. 2011, www.cdc.gov/motorvehiclesafety/seatbeltbrief/index.html.

Privacy Checkup Google. (n.d.). Retrieved from https://myaccount.google.com/privacycheckup?utm_source=google&utm_medium=hpp&utm_campaign=q12020-pcu&pli=1

Sanders, J., & Patterson, D. (2019, July 24). Facebook data privacy scandal: A cheat sheet. Retrieved from https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/

Sawaya, S. (2020, January 27). Cisco Study: Businesses Must Pony Up on Data Privacy. Retrieved from https://www.sdxcentral.com/articles/news/cisco-study-businesses-must-pony-up-on-data-privacy/2020/01/

Statt, N. (2020, March 24). Apple updates Safari's anti-tracking tech with full third-party cookie blocking. Retrieved from https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking

Strycharz, J., van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 13(2), Article 1. https://doi.org/10.5817/CP2019-2-1

Tarran, B. (2018, May 29). Royal Statistical Society Publications. Retrieved from https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2018.01139.x

The Associated Press. (2016, September 28). Half of MN law enforcement users misuse database searches, audit finds. Retrieved from https://www.twincities.com/2016/09/28/audit-half-of-minn-law-enforcement-users-made-questionable-database-searches/

The History of Seat Belts: Have They Always Been Effective for Men and Women? (2020, April 9). Retrieved from https://saferide4kids.com/blog/history-of-seat-belts-effective/

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. Journal of Marketing Research, 50, 546-562. https://doi.org/10.1177/002224371305000501

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. Journal of Marketing Research, 50, 546-562. https://doi.org/10.1177/002224371305000501

Wordtracker. (n.d.). Retrieved from https://www.wordtracker.com/search?query=data privacy

Zawacki, T. (2019, May 6). Why Consumers Prefer Personalization. Retrieved from https://multichannelmerchant.com/blog/why-consumers-prefer-personalization/