Evolution of Privacy, Data Policy & Internet Advertising in the United States

By

Tatiana Baughman

Supervised by

Prof. Caroline Le Bon

Submitted to the Washington College Department of Business Management in partial fulfillment of the requirements for the degree of Bachelor of Arts

Date: April, 10, 2020

Washington College Honor Code

I pledge my word of honor that I have abided by the Washington College Honor Code while completing this assignment.

Tatiana Baughman

Abstract

As technology has evolved, so have privacy policies and regulations. The internet is a limitless domain where both users and companies can provide and access information. Corporations and their partners have taken advantage of the internet to network and connect with users by collecting personal data, and targeting individuals with personalized advertisements. Despite many citizens showing concerns over privacy, there is still complacency among people to inform themselves about their rights, and a lack of direct communication between users, and companies. Through an analysis of the historical context of current political and business policies, and of social and technological evolution, I make three recommendations for better user-business relations that would ultimately lead to a safer internet environment.

Table of Figures

Table of
Contents

Introduction

How much information do you share on the internet? Which platforms do you choose to spend your time on, and how many ads are personalized to you? Do you know how much information about you Internet Service Providers, social media platforms, and third parties store? This thesis will focus on data collection, consumer privacy, federal regulation, and online advertising in order to examine relationships between practices and expected means of privacy. Chapter 1 discusses the history of data collection and federal policy within the United States. This section serves as the basis for readers to understand the evolution of governmental regulation and business policy regarding technology and data collection. My overview begins in 300BC in the Library of Alexandria, representing how early humans — such as Alexander the Great — craved knowledge, collecting information to store in his library. Readers are then brought into the 1660s when John Graunt first executed statistical analysis to connect previously recorded data with economic decline after the Plague. Afterwards, readers continue walking through history to understand the government's increasing interest in data and the value it has.

As technology became more sophisticated and more widely available to consumers, issues of privacy became more pronounced, which can be seen throughout the 1960s. The emphasis on fair practices by companies, regarding consumer privacy and company policy, even led to the creation of the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC). Issues of privacy and data collection have influenced federal regulations through a variety of legislation such as the Privacy Act (1974), the Computer Matching and Privacy Act (1984), the Child Online Protection Act (1988), Children's Online Privacy Protection Act (1998), the California Consumer Privacy Act (2018), and the General Data

Protection Regulation of the European Union (2018). But as of yet, there is not a single, overarching federal law regarding user internet information privacy.

In Chapter 2, readers will explore the beginning and interworking of the internet in a broad scope specific to the internet and the ISPs that give users access. There will be an increasingly targeted look into the online realm that harbors search engines and edge-providers. It is important to analyze various internet actors to understand the relationship between them, and how they each collect and share user data through cookies, third parties, and other means. Analysis of the advertising industry in Chapter 3 will reveal the importance that particular companies place on online ads and their methods of targeting advertisements toward particular groups or consumers via previously collected data. Chapter 4 discusses general privacy perceptions consumers have when on the internet, and their interactions with particular platforms. Many consumers are not fully aware of the extent to which businesses collect information or how they use it, transitioning us onto the subject of social media. Social media, generally speaking, is a digital platform or community created to allow the sharing of ideas and connecting people. This section describes who the main users are on social media, for what platforms are typically used, and why advertising is important to these sites.

In the following section of Chapter 5, I tie together privacy, social media, data collection, and advertising, focusing on particular companies such as Facebook and Google as well as their distinct privacy policies. Finally, I present my recommendations, which encourage consumers to be actively aware of the information they share on the internet and to understand how their information is collected and used by corporations as well as the potential risks that result. Furthermore, I recommend that there is a need for a comprehensive, carefully worded federal privacy policy because one does not currently exist. Such a policy would help set a baseline

expectation standard for all companies, resulting in easier regulation. A federal policy would also be feasible, particularly for large corporations to follow, as many already follow the guidelines of the GDPR. My final recommendation is for corporations to take responsibility for clarity and transparency with their consumers about the information they collect, analyze, and share. They must request explicit permission and find ways to communicate their intentions with consumers directly. Adaptation of these recommendations would build trust between consumers and businesses, producing increased customer loyalty and retention, as well as inspiring a safer internet experience.

Chapter 1: The History of Data Collection and Federal Policy in the United States

I will begin by discussing the history of data collection and how U.S. technology and policy have impacted the way we collect data today. Prior to the development of technology and computers, verbal communication and hand scribing were the only ways to record information. These were the manners in which individuals could conserve traditions, history, and culture. Consider, for example, the first attempts at mass storage by using the abacus in Babylon circa 2400 BCE (Marr, 2015) or the Library of Alexandria (300BC - 48AD). Humans always had a thirst for information and have always developed ways to record and preserve the traditions of their respective cultures. Alexander the Great craved the expansion of the European in pursuit of newfound knowledge which was eventually protected in the Library of Alexandria (El-Abbadi, 2019). A few centuries later in the 1660s, John Graunt executed statistical data analysis regarding the bubonic plague and the mortality data which revealed trends between English mortality rates and economic trends. Gaunt's friend, Sir Thomas Petty, found a correlation between Graunt's statistical data and the economic decline (The Editors of Encyclopedia Britannica, 2019). Moving forward to the 1860s when Richard Millar Devens uses the term

"Business Intelligence," referring to how businesses use data analysis for business purposes, in his "Encyclopeadia of Commercial and Business Anecdotes" (Marr; Foote, 2017).

The early United States government of the 1880s relied solely on pencils and paper to record population statistics. The U.S. Census Bureau asked only a small grouper of questions that tended to be not very specific to census takers, which proved to be an issue within local government functions as the ability to process and publish data efficiently was complicated. "But as the country grew, and policy and business leaders began to recognize the value of census data, questionnaires became longer and tabulation necessarily became more involved" (U.S. Census Bureau, n.d.). By the 1950s, data computing was becoming increasingly valuable with the use of big, mainframe computers like the IBM model #7074, which the IRS used for tax collection (Cappello, 2017, p. 178). Although Lawrence Capello argues that a reduction in privacy and an increase in data collection dates back to the Eisenhower era, data collection has been around much longer, as seen through the aforementioned history. Currently, modern technological studies show growth and sophistication, but it appears as though many choose to leave information responsibility for businesses, merely commenting on how individual's and private companies' grand-scale data collection is simply a "byproduct of technological revolution" (Cappello, p. 178).

Moving forward on the historical data collection timeline, it is important to note the strong political influences on data policy that was catalyzed by the rise of new machines. According to Capello, "New Deal liberalism played the greatest role in the unprecedented expansion of data collection in the U.S." (2017, p. 179). This is to say that westward expansion, the push for progress and innovation in combination with the conservative pressure for smaller government and more control for the people, led to the need for data collection as a means of

efficiency. Helen Nissenbaum, a professor of information science at Cornell Tech, agrees that the "democratization" of computers and technology allows smaller companies and people access to information (p. 38), decreasing individuals' control over privacy. The topic of individual privacy became of increasing concern with the modernization of new technologies relative to governmental and corporate monetary ability. Subsequently, the standardization of modes and methods permitted private businesses and individuals to access information (Capello; Nissenbaum, 2010). Helen Nissenbaum writes in her book, Privacy in Context: Technology, Policy, and the Integrity of Social Life, that the advancement of scientific fields and areas of mathematical study allowed for "information [to] be compressed, sorted, manipulated, discovered, and interpreted as never before, and thus… more easily transformed into useful knowledge" (pg. 37).

While what would become the "internet" was eventually upgraded and enhanced in the 1970s by Robert Kahn and Vinton Cerf (Andrews, 2013), the 1960s housed many debates regarding computer advances and threats to privacy. In contrast to free-market ideologies, and in conjunction with subtle changes within social and political realms, information was becoming increasingly more valuable. It was discovered that the Federal Housing Administration was selling each report for $1.50 to mortgage concerns for credit loan applicants (Allen, Scott, 1966). The increase in "aggregate data" and sharing information across government agencies and private companies sparked expanded interest in the value of consumer data and business practices. Capello writes that "American corporations, as well, used data gleaned from government agencies and other companies to make their direct-marketing campaigns more sophisticated" (2017, p. 184).

The Lewiston Daily Sun published a paper in 1966 that covered a range of topics, including the recommendation by a White House task force to establish a federal data center which would hold comprehensive information on military service, IRS information, census data, medical records, credit, criminal reports, and Social Security information relative to each person in the United States. This proved to be a highly controversial area, not only regarding personal privacy and positions of power but also legally, because certain documents are not legally accessible without an individual's consent. One of the arguments against having a large database came from New Jersey Congressional representative Cornelius Gallagher, head of the Subcommittee on the Invasion of Privacy, who stated that the database "could constitute a highly dangerous dossier bank" (Allen, Scott, 1966, p. 11). It would be only a year later that the Freedom of Information Act came to pass, "dramatically reforming public access to government records" (Solove, 2006, I-24). This Act allowed for any individual to freely request the records of stored government information about themselves without a need or reason to do so. The public freely having a route to their collected information increases transparency and lessens the disparity of access to information, unless it falls under one of the nine exemptions which FOIA.gov describes as protecting "interests such as personal privacy, national security, and law enforcement" (n.d.). This was an important precedent set by the government as each of the 50 states has a version of the Freedom of Information Act in place within the state level (Solove).

A few years after FOIA, and preceding the Watergate Scandal, is the publication of the HEW report by the Department of Health Education and Welfare (Capello, 2017; Solove, 2006). The HEW report alerts that individuals may unknowingly relinquish information to "large and relatively faceless institutions, for handling and use by strangers — unknown, unseen, and, all too frequently, unresponsive" (DHEW, 1973, p. 29). It also discusses the benefits and potential

woes that come with technological data storage, the potential misuses, and how citizens should have direct access to their records via institutions, the right to restrict access, accompanied by the ability to change the record if the information is not correct. The HEW report also denounces any secret databases of personal information and any manners in which citizens would be forced to divulge information. Thus, came the Privacy Act of 1974.

The Privacy Act arose from increased public attention and concern primarily generated from the HEW report. The Act itself derives much of its content from the HEW report, but not all. It allowed people to access and correct their information, yet also "placed restrictions on the collection, use, and disclosure of personal information by federal agencies" (Capello, 2017, pp. 187-188). There were some issues with this Bill as it carried a "routine use" exemption and did not apply to local or state records, nor private companies. This loophole allowed the "disclosure of personal information" if the use of said information by the government matches the purpose of disclosing the information (Capello; Solove, 2006). Data has been, and will always be, valuable information for companies and the government.

During the 1980s, the U.S. government federally sanctioned data mining, thus both public and private companies began sharing information by using techniques, such as "data matching," or "cross-referencing," the process of comparing multiple digital records. The Reagan administration worked diligently toward a smaller government, resulting in the expanse of "private interests who benefited from access to government data," as Lawrence Capello writes (2017, p. 180). "Data matching" gained a reputation as a money saver that enhanced bureaucratic efficiency, and throughout the 1980s, states implemented their own matching programs" (p. 189). Data mining was a huge money saver for the government and companies, illustrated during the Reagan administration. The Reagan administration's "SPECTRE" project matched Social

Security numbers with death records to verify that the correct people were receiving benefits. As it was discovered, the HEW report stated that there were about $7.5 million in recoveries for trust funds and overall savings of $25.3 million (Capello; DHEW, 1973), meaning that the HEW report exposed many people who were fraudulently collecting benefits on dead relatives. This revelation fueled the privacy dialogue and brought attention to the actors with access to sophisticated information.

The conversations and debates surrounding the topics of data and privacy ultimately led to fewer permissions given to institutions, such as the legitimacy of collecting information about people (Capello, 2017). As a result of public apprehension, the government passed the Privacy Protection Act regarding subpoenas in 1980, and in 1988, the Computer Matching and Privacy Protection Act (CPPA). The CPPA addresses the loophole in the Privacy Act regarding the "routine use" exception, but it does not eliminate the exception. Instead, it permits guidelines for the computer matching process that many companies used, inspired by the government using this process within their internal structure (Solove, 2006). Lawrence Capello writes, "[the Computer Matching and Privacy Act] also effectively legitimized computer matching as a desirable part of American life, institutionalized the routine sharing of information between agencies, and created the de facto national data center privacy advocates had opposed for decades" (p. 192). Computer use and access were becoming more commonly available, leading people to alter how they chose to intake information and sustain records. Online access and data storing would alleviate the need for individuals to keep mental receipts of informative materials but would open the door to new ways of communication.

Scholars agree that there is no need to rely on human memory and storytelling (Nissenbaum, 2010), because people no longer need to physically search through paper

documents and files to find information, instead accessing them via home computers. Let us not forget that to find this information, there must first be internet accessibility, and in 1989, Sir Tim Berners-Lee provided the global platform. While working in the European Particle Physics Laboratory at CERN (The European Organization for Nuclear Research), Sir Time Berners-Lee created the world wide web as a global platform available for all people in 1990, writing the first server and web client (Internet Hall of Fame, n.d.). Not only do consumers, individually, have access to information and different forms of communication, but now companies have a new method to record data for their uses via "cookies" and tracking "click-stream" data (Solove, 2006). Packages of information stored on a user's hard drive of their computers, between parent site visits, are called "cookies." As a user returns to the parent site, the "cookie" is searched for to collect the harvested information. "Click-stream" data refers to the path a user follows when they enter a website domain. "Clickstream analysis" (also called clickstream analytics) is the process of collecting, analyzing and reporting aggregate data about which pages a website visitor visits — and in what order," writes Margaret Rouse (n.d.). Companies like Google and Facebook use this information to better personalize content for their users via advertisements or platform design/interaction.

The creation of the world wide web did not harbor any limitations to content, such as age restrictions. Therefore, to protect youth data and information on the internet, the Children's Online Privacy Protection Act (COPPA) of 1998 was formed. The application of this Act applies to "operators of commercial websites directed to children 12 and under that collect or maintain personal information, as well as other websites that have actual knowledge that they are collecting or maintaining personal information from a child 12 and under" (FTC, 2002).

COPPA requires companies to post a privacy policy on the website, notify, and acquire parental consent for use of their child's information. COPPA also allows the right for parental review and revocation of consent and must establish reasonable and maintainable procedures for future processes. This Act appears to be, mostly, successful as the FTC (Federal Trade Commission) reports in a survey on compliance. In April 200 — a year of implementations — 90% of companies were providing a privacy policy, "that said whether the site collected personal information, how the information was used, and whether the information was shared with third parties." Still, there were other areas where corporations did not meet all the other requirements, such as not notifying parents of their ability to review the collected information (FTC).

COPPA was an attempt to protect individual privacy directly for children under the age of thirteen, but after the September 11 attacks in 2001, privacy became less of a concern and data collection methods strongly increased, particularly by the government. There was high tension after 9/11 which led to the government requesting company information about their customers and clients from other corporations (Solove, 2006). One example is the flight industry. Post 9/11 saw government requests for informational studies to supplement airline security studies. Northwest Airlines adhered to the government's request and, unbeknownst to their clients, "provided NASA with the names, addresses, credit card numbers, and travel itineraries of persons who had flown on Northwest Airlines between July and December 2001" (Dyer v. Northwest Airlines Corporations, 2004). Although there was push back by consumers about the sharing of their information, the courts dismissed the case.

Each passing year, there is more and more advancement in the technological realm. More data and modes of transferring and capturing information mean that there must be systems and

regulations in place to better protect peoples' privacy. If this cannot happen, and the systems in place are not strong or structured enough to protect this data, then individuals will be more reluctant to trust companies with their information, which could result in economic mayhem. Daniel Solove writes about the 2005 data breaches of several data brokers. One example he uses is of the ChoicePoint company which "sold personal data on over 145,000 people (the figure was later revised to 162,000) to fraudulent companies established by a ring of identity thieves" (Solove, 2006, I-45). As another example, the information provider LexisNexis also suffered data leaks and break-ins. How are Americans to put their faith in companies after data breaches, and how do business practices adjust to assure people their information will be protected? What is "user privacy" on the internet, and how do individuals protect themselves?

In more recent years, states have adopted a legal policy concerning privacy and data collection. California is one of the most recent states, adopting the 2018 California Consumer Privacy Act regarding personal data collected by businesses that foster new consumer rights for access, removal, and sharing of information (Office of Attorney General Xavier Becerra, 2020). Every state now has regulations in place regarding privacy to an extent (Raul et al., 2019), but each law is different. So, to reach cohesive rules and regulations, it may be worth the adoption of federal privacy law similar to what the European Union did in 2018. The European General Protection Regulation (GDPR) was adopted to protect consumer privacy information collection and processing by organizations. The regulation also gives users the right to be informed about the uses of their data (GDPR, 2018; Long et al., 2018), but also the right to opt-out, revoke access to, or have companies delete information about them. Some key issues covered in the GDPR are:

- Consent

- Fines / Penalties
- Personal Data
- Privacy by Design
- Privacy Impact Assessment
- Right of Access
- Right to be Forgotten
- Right to be Informed

It is a very comprehensive piece of legislation covering many areas of data collection, personal privacy, and the access/limitations that actors have to personal information within the internet.

Chapter 2: Internet Actors & Their Functions

The FCC, FTC

In order to comprehend what "user privacy" is on the internet, it is important to understand who the FCC and FTC are, what roles they play, and the differences between ISPs (Internet Service Providers) and edge providers. The FCC is the Federal Communications Commission. It is independently overseen by the government and regulates both international and in-state communications throughout the states and the U.S. territories, whether that be by radio, tv, wire, satellite, or cable. The FCC stands for:

- "Promoting competition, innovation and investment in broadband services and facilities
- Supporting the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution
- Encouraging the highest and best use of spectrum domestically and internationally
- Revising media regulations so that new technologies flourish alongside diversity and localism

• Providing leadership in strengthening the defense of the nation's communications infrastructure" (FCC, n.d.)

On the other hand, the FTC, or Federal Trade Commission, was created in 1914 by Congress as an authoritative grouping to oversee fair trade market practices and curtail any unfair methods of competition in commerce (FTC, n.d.). "Federal and state authorities, as well as private parties through litigation, actively enforce many of these laws, and companies also, in the shadow of this enforcement, take steps to regulate themselves," as Alan Charles Raul, Christopher Fonzone and Snezhana Stadnik Tapia writes in Chapter 26 of the Privacy, Data Protection, and Cyber Security Law Review of 2019 (pp. 1-2). In summation, the FTC aims to protect consumers while also promoting competition by analyzing complaints, ensuring companies follow the law and their privacy policies, and making sure both businesses and people are educated about their rights and responsibilities (FTC).

These practices are found in section 5 of the FTC Act, which was the genesis for the action brought against Sears in 2009. The FTC had to step in when Sears allegedly neglected to disclose proper information to their consumers about the data they were collecting. This government entity seeks to also protect personal data as it stands against the collection of "personal data in ways that are materially different from, and less protective than, what it initially disclosed to the data subject," without receiving consent from the parties to whom it may concern (Raul et al., 2019, p. 402). In many cases regarding the disclosure of data collection between companies and their consumers, the FTC has played and continues to play a large role in the transparency of corporate surveying and tracking methods. "The FTC has not, however, indicated that opt-in consent for the use of non-sensitive information is necessary in behavioral advertising," a topic that will be discussed in later chapters (Raul et al., 2019, p. 402).

Internet Service Providers (ISPs)

Relative to the digital platform (i.e. the internet) are Internet Service Providers, or ISPs. This references companies such as Verizon, Comcast, or Delmarva Wi-Fi which charge users money to access the internet. “Edge providers,” by comparison, are the companies within the internet that offer services for users, search engines like Bing and Google, streaming networks such as Netflix and Hulu, online shopping like Amazon, or social media sites like Facebook, Twitter, Instagram, YouTube, etc. (Nasr, 2016). It is important to note the differences between platforms as to how they collect user data are not the same. It seems that a majority of people and media tend to focus on social media platforms that access your information. In reality, the much larger threat to your information is your Internet Service Provider. Check the privacy page(s) of your provider to see what information is available to them and what they compile. Verizon’s privacy policy, for example, explains the different categories and areas of information gathered such as credit information, location, and demographics. Verizon also tracks social media information such as likes and other interests when you “use your social media login to interact with Verizon sites or offers” (Verizon, 2020). Verizon states that they use all this information to cater services and experiences to their consumers, and as a means to check credit, verify identity, and research/develop new products, but they also share information with third parties. In terms of advertising, Verizon states, “We will obtain your affirmative consent before using information about your visits over time to different non-Verizon websites to customize ads specifically to you. One such program is Verizon Selects” (Verizon). There are a variety of ways that users may opt-out of these data collection practices or control what information they are providing, but each opt-out process has its own set of measures to follow which may incentivize people not to follow through as each process may be long or tedious.

Comcast, on the other hand, provides transparent information about their Xfinity privacy policy on both the Xfinity and parent Comcast sites. Comcast states that they do not collect, share, sell, or buy information about their consumers. The only information given to third parties or others is solely to complete their duties for the consumer, and those parties are not allowed, by Comcast Contract, to share said information (Comcast, 2020). In summation, ISPs are the broad overarching companies that allow access to the internet via a subscription or monthly/yearly fee (Csokasi, Moody, 2019). It is important to note that various websites and providers have differing policies, so when moving around the internet, one should have an awareness about the potential collection of your information. Furthermore, it is also the consumer's role to make sure they are aware of the conditions for their privacy and information, and the rights available to limit company access to their materials. In 2016, the FCC proposed regulations that would limit the amount of access that an ISP would have to its consumers. In contrast to the FTC rules and regulations about explicit opt-in consent for a limited amount of personal information, the FCC proposal requires a much broader basis for opt-in consent, such as requiring opt-in consent for all uses of consumer information. The FCC's plan aims to "cover the broadband providers, while the FTC would deal with internet companies on the front end such as Facebook or Amazon.com" (Nasr, 2016). Nasr's statement is important in its allusion to Facebook and Google, referring to applications otherwise known as "edge providers." These actors have different methods of data collection than those of ISPs since they are not privy to as much diverse information which ISPs may receive.

Edge-Providers

As previously mentioned, Facebook, Amazon, and corporations of similar structures are considered "edge-providers." These companies are the platforms within the internet realm which

are accessible via an internet service provider. This "means an individual or entity that provides any content, application, or service over the Internet, or an individual or entity that provides a device used for accessing any content, application, or service over the Internet" (Law Insider, n.d.). Each website has its own set of privacy policies, terms of use agreements, and cookie policies, but each of the 50 states also has particular policies that must be adhered to as well (Raul et al., 2019).

Since enactments of laws and regulations through Congress, companies have been forced to adapt to new ways to collect data to use for their business purposes, including being more transparent. Why do corporations spend so much time collecting your information and why is it so valuable, one might ask. Data is used as a means to target consumers via promotions of products and services, to help business systems and processes with their efficiency, and the ability to turn a profit.

The Washington Post authors Brian Fung and Craig Timberg mention that the acquisition of AOL and Yahoo allows them to double charge users for working with those platforms (2016). If a business can figure out which individuals are interacting with its websites and products, and how people are interacting with them, then the business can formulate plans and processes to better meet the needs of their consumers allowing them to form advertisements, promotions, and deals specifically directed at customers. It may also be a consumer advantage to receive only tailored offers and promotions. As mentioned before, cookies are a primary way in which a site can compile data, but third parties are another method and group interested in user information. Third parties are any other source, other than the website an individual is intended to be on, that receives and harbors consumer data (Curac-Dahl, 2019). Third parties themselves are "other embedded websites that your browser also talks to such as advertisers, website analytics engines,

or social media widgets — that can observe your browsing behavior" (Urton-Washington, 2016). The Privacy, Data Protection and Cyber Security Law Review (2018) discusses a variety of countries and their interaction with, or regulation of, technology. These authors discuss how third parties are given access to information despite not maintaining proper disclosure mechanisms, nor receiving explicit consumer consent, regardless of the safeguards put into place by the FTC. In a study entitled "Behind the scenes: a cross-country study into thirdparty website referencing and the online advertising ecosystem," authors R.C. Nurse and Buckley found that the United States is the country with the highest amount of internet users (2017). Their study indicates that there is quite a bit of information to be tracked and distributed. Nurse and Buckley's study examines 250 websites within the UK, USA, Germany, Russia, and Japan as a means to better understand user perceptions of privacy, and the eco-web system interactions between main websites and other parties involved, such as third parties. Third parties such as Google Analytics or Double-Click, both of which are owned by Google, tend to have some of the largest involvement in the online realm (R.C. Nurse, Buckley). Present-day, multiple third parties are viewing a single user's interactions and gaining insight into their likes and trends, which they can provide to companies who want that information (Urton-Washington, 2016).

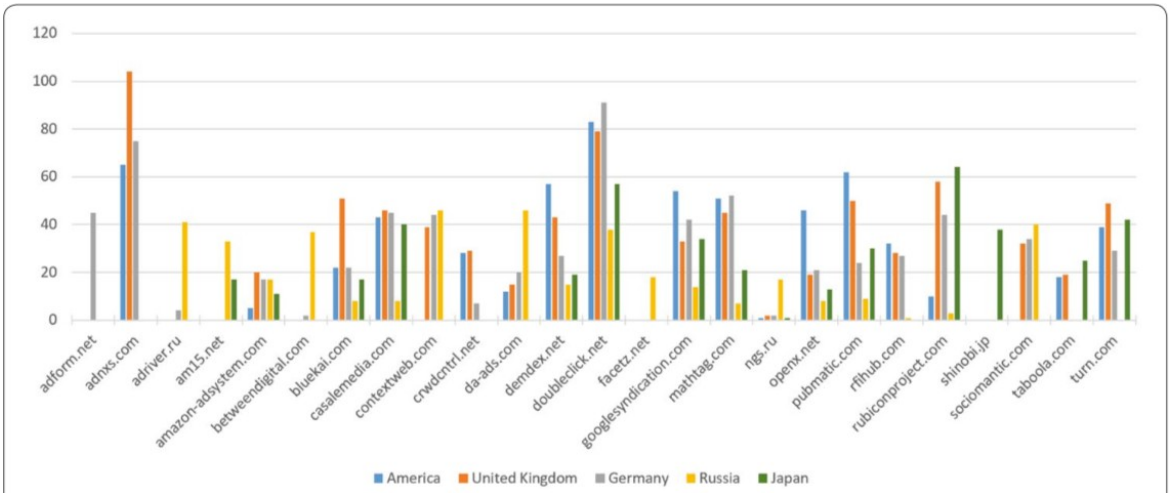

Fig. 5 A comparison to show the number of references made by each of the third-party websites, across the five countries that were studied (USA, UK, Germany, Russia and Japan)

Figure 1. (R.C. Nurse, Buckley, 2017 p.11)

Over the years, better ways of tracking user behavior have developed, and although cookies were the primary manner for a long while, it has evolved even further to track more specific details such as "screen resolution, time zone or the availability of specific font sets" (R.C. Nurse, Buckley, 2017, p. 3). R.C. Nurse and Buckley elaborate, "common activities include leveraging big data to optimize digital marketing and developing approaches to extract individual user profiles from online surfing information for purposes of behavioral targeting" (p. 3). This allows users to be identified on a variety of different sites, leading to more accurate profile building and user data collection. Figure 1, above, shows the amount of "references" or other web point connections that were made between third party systems among five countries. Advertisers are interested in third parties because they can exchange information with them to target content toward online users.

Chapter 3: The Online Advertising Industry

Although cookies and tracking systems are used for a variety of reasons previously mentioned, for this thesis, the primary focus of data collection discussion will be regarding online advertising. Primary websites and third parties work in tandem to gather information as a means to better target advertising, products, and services toward their intended target markets. Rudikowa et al. states: "Currently, an increasing number of researchers are using big data to evaluate numerous aspects of human activity, including human relationships in different social networks" (2019, p. 195). The online advertising industry is massive and only continues to grow as technological advances are made. "U.S. digital advertising revenues reached $57.9 billion during the first six months of 2019 — the highest spend in history for the first half of the year — according to the latest IAB Internet Advertising Revenue Report released by IAB and prepared by PwC US" (IAB, PwC, 2019). Figure 2, below, visually shows the increase in advertising

revenue generated from 1997 - 2019.

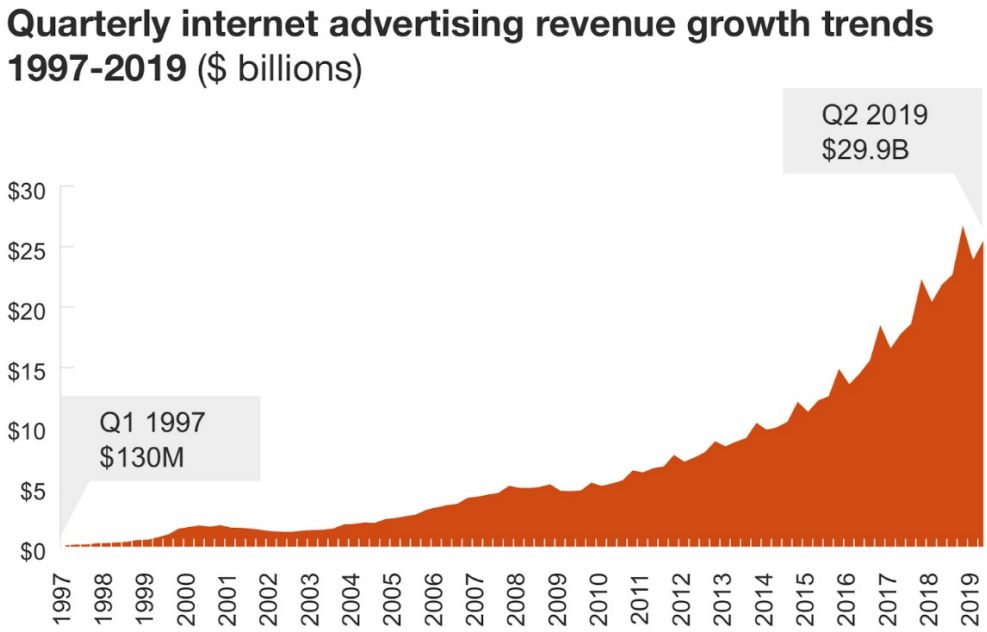

Figure 2. (IAB/PwC Internet Ad Revenue Report, HY 2019)

Even though digital advertising is currently the largest area for ad revenue, companies continue looking for new strategic methods to advertise to consumers, relying on channels such as video games, virtual realities, or TV subscriptions (IAB, PwC, 2019). Digital advertising is a method of engagement by advertisers to gain recognition and interaction with a brand, product, service, etc. Advertisers can choose on which platforms to buy advertisement space and determine what sort of marketing approach they think would be best to reach consumers. There are a variety of different methods in which they could portray an ad through visual appeals and content, but the particular type of social media account and respective environment must be carefully considered. Each platform has a community and a perception that could potentially influence, or "prime" the individual in the way they interpret the advertisement (Dahlén, 2005; Voorveld et al., 2018). Therefore, when advertisers are gathering information via cookies and third parties, they also take into account other factors that could lead to higher user engagement. Behavioral advertising

is very common and popular within online advertising, because it is the process of placing ads for particular users "based on information collected on each user's web search and browsing behaviors" (Yan et al., 2009). Advertisers can subsequently gauge ad success typically through the advertising revenue, or the CTR (Click Through Rate), that is, the ratio of users who click on links to numbers of users who view the ad. This is said to be one of, if not the main method of, online advertising in its effectiveness. "However, the practice also involves collecting, using, and sharing personal data, and thus raises consumer privacy concerns" (Boerman et al., 2017, p. 363). As a result, advertisers and other sources, such as third parties, collect an immense amount of information and it circulates the online web. This can include but is not limited to purchases, searches, videos watched, emails sent, ads clicked, and websites visited (Boerman et al.). As access to personal and sensitive information is accumulated by these means, how are users able to protect their privacy on social media and online platforms?

Chapter 4: Privacy + Social Media

The notion of privacy itself is a "multifaceted concept" (Capello, 2017, p. 178). Each person has a right to privacy and their expectations of what it might consist. In terms of the online realm and social media use it is "the control of who has access to information about the self" (Zurbriggen et al., 2016, p. 249). This topic has been an area of concern since advanced technology, data storing, and communications were emerging, which can be seen through all of the historical innovations and political policies that were examined in Chapter 1. Over time, it seems that people have become more concerned with keeping certain information from public knowledge. Considering all the means, methods, and modes in which citizens can interact and share information at any moment, increasing public concern makes sense. It also makes sense relative to corporations and businesses. It was previously discussed that companies desire data

for a variety of reasons, but mainly to help their business processes to some degree. Businesses also use data to understand their consumer base to a great enough degree in order to build advertising campaigns and implement them on platforms in ways that will engage their consumers to generate the company revenue. The next section will explore privacy as an online concept that relates to consumer perceptions versus revenue streams for companies. It will then discuss particular companies, their policies, and particular privacy issues in the past, especially in ways they relate to social media.

Social media is largely defined as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0 and allow the creation and exchange of user-generated content" (Kaplan, Haen-lein, 2010). Now it is possible to break "social media" into particular categories like blogs, gaming sites, etc., but our focus will be on social networking sites (edge providers), such as Facebook, Instagram, and Twitter, and search engines, such as Google and Bing. Primarily, these are all spaces for content to be found, shared or created, and platforms to build connections with others.

Since 2019, the amount of social media users in the United States increased by 2%, bringing the number to about 247 million people with online profiles. Facebook lead in user activity (Clement, 2019; Zurbriggen et al., 2016). User percentages can be seen below in Figure 3.

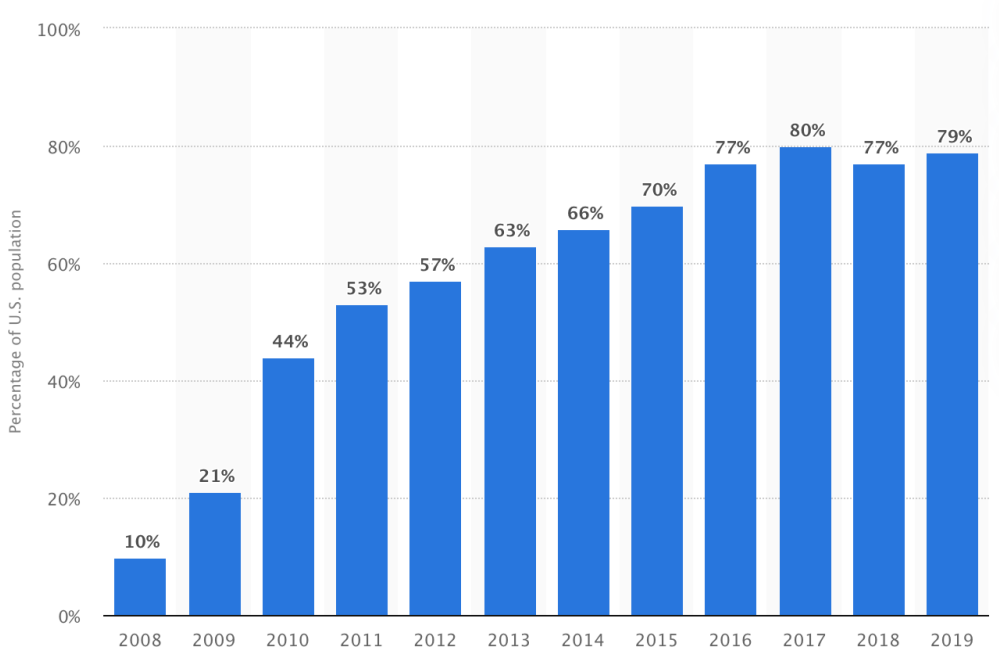

Figure 3. (Clement, 2019)

Of this large portion using an online platform, it tends to be the younger generations — ages 18-29 — who use social media platforms as opposed to those who are 65 or older. Facebook was the leader in sharing content whereas Instagram led with photo sharing (Clement). So, why do so many people use social media sites? Social media allows a common online space in which individuals can share and express whatever information they choose as a means to connect with an electronically based community (Alhabash et al., 2017). People are given the freedom of expression, within community guidelines, and may choose to share information that may shape public perceptions. Figure 4 shows the various manners in which people engage with the online realm within the United States population. About 87% of the U.S. population is active on the internet.

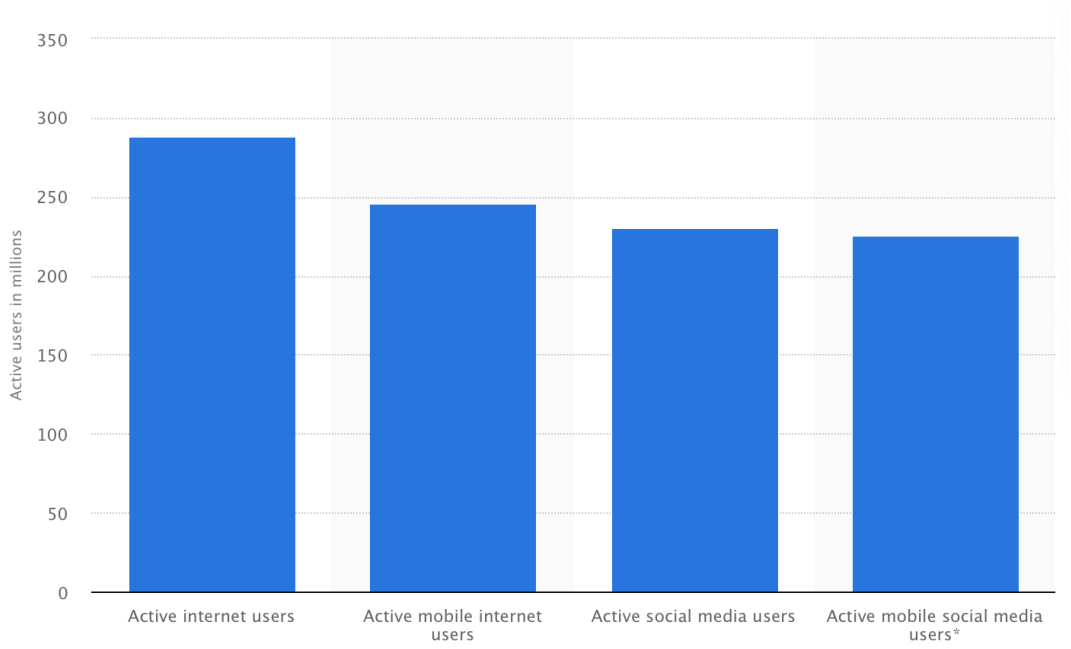

Figure 4. (Clement, 2019)

With such a large percentage of people on the internet, companies and advertisers have a considerable opportunity to build connections with their consumers, hence the percentages of ad spending by companies in Figure 5. It is also a cheaper means of reaching many people and can tell a lot about the consumer via tracking likes and interests (Rudikowa et al., 2019). Stronger efforts are being made to influence behaviors and increase competition for consumer support and loyalty. Advertisers want to drum up interest, so they may use online influencers, pay for promotions, or brand ambassadors. This is particularly successful when advertising stems from friends or trustworthy faces making advertisements less "ad-like" than a banner or single promotion (Alhabash et al., 2017).

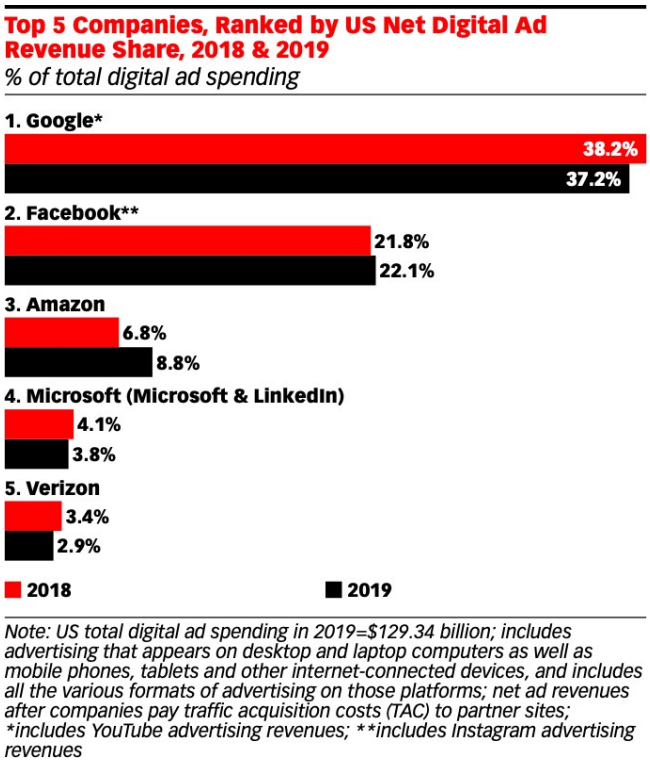

Figure 5. (eMarketer, 2019)

Alhabash et al. defines social media advertising as being "any piece of online content designed with a persuasive intent and/or distributed via a social media platform which enables Internet users to access, share, engage with, add to, and co-create" (2017, p. 4). Therefore, if advertisers are implementing various methods as a means to gain customer involvement and influence behaviors, how are people truly to believe in their online autonomy? The online realm can be very volatile which can negatively impact personal privacy, whether friends share information and tag you in a post, your face is automatically recognized in photographs as on Facebook, third parties/host websites track credit card information, demographic data, or likes and dislikes. So once again, what particular measures should individuals take to protect the information they do not want to be tracked, scanned, or shared within the business realm? I will address this question in the following sections.

Chapter 5: Privacy Protections & Company Policies

It is said that users want to feel as in control of their privacy as possible, and have the freedom to divulge information on their terms (Zurbriggen et al., 2016; CHO et al., 2019). Social media platforms are communities whereby other users can share information that may involve other individuals, but for this thesis, "privacy" is being used relative to the individual. There are methods and manners in which consumers may go about protecting their privacy and limiting companies' intake or accumulation of information. Individuals may decide to install encryption software, ad-blockers, or Virtual Private Networks (VPNs) that protect a user's IP address (Namara et al., 2020). Another way to protect privacy is by adjusting the privacy settings on your accounts as settings can be adjusted from default positions to curb the general flow of information to companies and interested third parties. Additionally, a user might adjust ad limitation, location sharing limitations, or adjusting who can view your posts (i.e. Facebook's privacy filters on posts: "Only Me," "Friends except ___," "Friends," and "Public"). You can either allow or deny location sharing with apps to "Always," "Never," or "Allow while using." It is simply up to the user to make the effort to change their settings (CHO et al.). As the FTC would agree, it is the company's job to make sure that consumers are aware of the use of their information. Users must be aware of the freedom to change privacy settings and use the opportunity to potentially adjust all their privacy settings in order to better protect their information. Although, some consumers may also be more inclined to leave the default settings as an understanding of trust that the platform knows what is best or carries the consumer's privacy interests as a priority (McKenzie, et al., 2006; CHO et al.). Other than simply changing in-house privacy settings, or choosing opt-in, opt-out features, how many people truly take the

time to read the Terms and Agreements before accessing content, especially when the content is inaccessible unless you agree?

A 2016 study by Jonathan A. Obar and Anne Oeldorf-Hirsch regarding how many users read a full privacy policy before joining a website, showed that of the 543 people that signed up for the fake website "NameDrop," 74% skipped even reading the privacy policy, the average time users spent on the policy being only 51 seconds, and 98% missed the "gotcha clauses" put in place by Obar and Oeldorf-Hirsch. From their study, it can be seen that people, when faced with a choice between fast access and protecting their privacy, are more likely to trade their privacy for speedy entry (Obar and Oeldorf-Hirsch, 2016). N.Y. Times author Kevin Litman-Navarro produced an article after reading 150 privacy policies. He writes that the policies were "verbose and full of legal jargon — and opaquely establish companies' justifications for collecting and selling your data" (2019). People would need at least a college level or professional level vocabulary to comprehend the extensive documents which companies call their privacy policies (Litman-Navarro). Currently, many companies have made changes to their policies and consent information as they have come under fire federally and publicly for privacy breaches.

When people think about privacy, it would be safe to say that a majority of people primarily think of Facebook as it has been such an influential source of the new media over recent years. Primarily, the attention to information privacy began with the Cambridge Analytica scandal surfacing after the 2016 election. Cambridge Analytica was a data analytics firm that harvested information from more than 50 million user profiles from Facebook to inform political advertising strategies for the 2016 election toward particular users (Meredith, 2018; Cadwalladr, Graham-Harrison, 2018). This emergence of information left the public feeling betrayed and put

immense pressure on Facebook to revamp their privacy policies, which they have done a handful of times. One example of revision is when Facebook first "restricted its developer APIs [Application Program Interfaces] — which provided a way for apps to interface with Facebook data — in April 2018" (Nuñez, 2019).

What does all of this mean for Facebook advertising? Advertisers have over 200 modes to choose from in which they can target consumers through advertising on Facebook, and these "advertisers" need not even be verified companies, but may be ordinary individuals (Andreou et al., 2018). The importance of this must be recognized as Facebook has the highest amount of advertising traffic among social media platforms (Andreou et al.; Clement, 2020), and an extensive amount of the online community as Facebook members (Zurbriggen et al., 2016). Facebook's current advertising policy is concerned with a few areas:

- Activity across Facebook companies and products
- Activity on other websites and apps
- Activity with other businesses
- Location

Concerning specific advertisements, Facebook states, "Our ad system prioritizes what ad to show you based on what advertisers tell us their desired audience is, and we then match it to people who might be interested in that ad" (Facebook, n.d.). Facebook also affirms that consumer data is not sold to advertisers. Rather, third parties and partners have access to nonidentifiable data through the use of Facebook tools or widgets, such as the "like" button. Although Facebook does not sell data and information, they do receive materials from third parties for instance, "websites you visit or apps you use can send Facebook data directly by using our business tools (such as a pixel) to help us show you ads based on products or services you've

looked at, such as a shirt on a clothing retailer's website" (Facebook). Facebook users do have the opportunity to change their ad preferences, see why they are seeing a particular ad, and see certain information that advertisers and Facebook would be able to track, although it is argued how misleading this information could be (Andreou et al., 2018). Since Facebook is as popular and holds as much advertising content as it does, there are bound to be issues that arise. For instance, Facebook recently endured a $5 billion fine from the FTC over breaching a previous 2011 agreement regarding user privacy (Tracy, McKinnon, 2019). Furthermore, there has been turnover amongst the Facebook Board regarding the types of advertising allowed. As of March 13, 2020, Kenneth Chenault left the company, consistent with others who left the company due to Mark Zuckerberg's decision not to fact check political ads, as a commitment to free speech (Jeff Horwitz, Seetharaman, 2020). Instagram follows the same guidelines and regulations as Facebook since Facebook acquired Instagram in 2012 (Instagram, 2020). Advertising on social media is extensive, but how does it compare to a search engine?

Advertising on a search engine with as much span as Google opens many opportunities for advertisers to reach their intended consumers, but there is also potential for things to go awry. In 2007, Google acquire the advertising firm DoubleClick, which allowed Google to acquire the accounts of DoubleClick, giving more revenue to Google but also furthering its access to users. Google is a bit different than typical social media sites. As a search engine, it has more private access to people's thoughts, emotions, and specific interests as individuals turn primarily to the internet to search for answers (Tene, 2008). Search algorithms used by companies are unique for each business and are highly protected. In July of 2019, Australia announced that they were doing investigations into Google and Facebook due to the impression that these businesses have too strong of a hold on their news and media industry. "[The Australian Government] also found

many instances where companies had deprived consumers of control over their personal information" (Taylor, 2019). Google also faced a $5 billion antitrust fine from the European Union about Android phone systems. As a final example in regard to Google, and slightly aside from advertising with focus on consumer data, is the healthcare cloud storage campaign, "Project Nightingale." This project would consist of health information from over 50 million Americans to better serve doctors with health records.

Figure 6. (Copeland, Needleman, 2019)

Figure 6 shows how the system would work. Currently, the Office for Civil Rights in the Department of Health and Human Services has not found any HIPAA violations, but this idea will be watched considering how much identifiable personal and medical information will be stored in a cloud computing system (Copeland, Needleman, 2019). Most recently, with the COVID-19 outbreak, and the high demand increase for particular products such as N95 masks, there have been ads for these materials which fueled fears about the virus and, subsequently, lead

to a shortage in medical supplies for the actual medical community. Google said they would remove these advertisements which capitalize off the pandemic, because they go against the advertisement policy it recently put into place (Elias, Graham, 2020). Google's advertising policy outlines what advertisers are allowed to do and the content that is restricted. In terms of data collection and advertising, the company states, "We want users to trust that information about them will be respected and handled with appropriate care. As such, our advertising partners should not misuse this information, nor collect it for unclear purposes or without appropriate security measures" (Google, 2020). Similar to Facebook and Instagram, Google collects information about user location, device information, personal data, and more specifically:

"The information we collect includes unique identifiers, browser type and settings, device type and settings, operating system, mobile network information including carrier name and phone number, and application version number. We also collect information about the interaction of your apps, browsers, and devices with our services, including IP address, crash reports, system activity, and the date, time, and referrer URL of your request," (Google, 2019).

As you can see, Google has access to quite a bit of information. Users need to be aware of the information they are releasing and their options for limitation, and companies must be transparent and make sure they are protecting consumer data.

Recommendations

The realm of electronic data privacy in a world with constant innovation and push for financial prosperity makes it difficult to properly regulate and protect information online. Businesses want to take advantage of the platforms arising in their midst in order to make a profit and connect with consumers, and people want to connect to be social, follow trends, and

shop with ease. There has been a long history of technological innovation and privacy policies, laws and regulations put into place in the face of privacy debates. I would be remiss in stating there is a singular route that can be taken to automatically fix problems of privacy, but there seem to be a few viable options that should be considered in elevating the standards of privacy we have today. I recommend that users have a responsibility to themselves and others to be aware of the risks associated with online platforms, and be aware of the information they are sharing, which affects not only themselves but others. Next, legislation should be written with more clarity, and proper consideration given to adopting a federal privacy policy as the EU did when they implemented the GDPR. Lastly, companies owe it to their consumers to be clear and transparent about their policy partners.

As was stated before, the United States has the highest number of active internet users (R.C. Nurse, Buckley, 2017), meaning that people have chosen to participate in the online realm of information sharing and connecting. The extent of information shared, and with which specific parties, or for what particular purposes, are the questions of which most consumers are unaware. Many people are aware that their information, as stated in privacy agreements, is shared to a degree, and these individuals agree that they do have some amount of concern (Zurbriggen et al., 2016), but there is less action on their part to change access to their data (Preibusch, 2013). Individuals should understand that they have the right to limit the amount of information collected, and if they spend some time and effort to look at the privacy policies of particular companies or platforms, then they can better protect the information they do decide to share. If users take the opportunity, there are a variety of options to protect your location and information other than simply changing the default settings a company has in place. For example, users could research a variety of PETs (Privacy Enhancing Technologies) that would

shield them from others (Namara et al., 2020). People may also consider installing encryption software to secure browsers or VPNs (Virtual Private Network) to protect their IP addresses, ad blockers, or other programs. These protection measures can also be beneficial for those who may need to access sensitive information for work-related purposes, such as medical workers (Namara et al., 2020). It is important to note that with these methods, none are full proof, which is why people need to be aware of privacy policies and Terms of Use. Many people understand and will perhaps even anticipate that others can also share information about them, such as "tagging" people in posts (Such, Criado, 2018). It would make sense then to assume other humans will, in a social context, share information across platforms, but when companies do this with outside factors and third parties through monetary exchanges, it becomes an issue of privacy and legality.

In terms of legislation, wording is everything. Although there are Acts such as COPPA and the CCPA, the internet is large and expansive; therefore, it needs more specific regulation by states and companies to avoid loopholes such as the "routine use" exception in the Privacy Act. "Whole categories of data — like the customer and prospect databases widely used in sales and marketing — lack explicit protection under federal law, despite the fact that unauthorized access to them is potentially harmful to the data subjects" (Cobb, 2016, p. 6). Individual states are making moves to better protect individual data and privacies (Raul, 2019), but there are still places for improvement. All 50 states now have some sort of data and privacy policy in place (Raul et al., 2019), but it might be helpful to take note of the EU and the adoption of the GDPR (Leicht, 2018). Having a federal statute could potentially eliminate some of the gray areas and legal obligations, because the jurisdictions in internet legal issues are very broad due to the internet's "omnipresent nature," and the fact that "data is often transmitted across several

jurisdictions and rarely remains in only one" (Chiu, 2013, p. 291). Having this type of policy covering privacy and data collection on a broad spectrum would not be limited to only social media companies, but has the potential to encompass other fields that collect user data and information, such as phone companies and Internet Service Providers. Large corporations, such as those discussed previously, should be able to make this adjustment relatively easily since they already comply with the GDPR. Tim Cooke, CEO of Apple, even discussed his anticipation of such a regulatory statute for the U.S., saying "We at Apple are in full support of a comprehensive federal privacy law in the United States" (Baraniuk, 2018). Thus far, legislation has been very reactive to evolving technology; therefore, any piece of legislation that could be put into place would need to be carefully thought and discussed, but the primary areas that should be focused on are the types of consumer information allowed to be collected, notification requirements, opt-in/opt-out policies, and a standard framework to secure information (Chiu, 2013). Companies would, of course, have the responsibility of carrying out these duties diligently and effectively. Proper notification of information to consumers is perhaps an area that is most lacking by corporations. The FTC and the government have already been addressing companies that fail to follow their policies, such as taking legal action against Facebook and Google, but also by setting a legal standard as mentioned above, giving smaller companies the incentive to create better practices of informing their consumers. For instance, the U.S. could look to the EU as a privacy example, "for businesses and consumers that are engaged in the transfer of personal data that is based on 'comprehensiveness'" (Chiu, 2013, p. 306). More companies could follow Google, Instagram, and Facebook's lead in offering a "Why am I seeing this ad" feature that could offer direct advertising information to consumers (Andreou et al., 2018), or the pop-up cookie tracking notification that currently appears on a vast amount of websites already. That

being said, there is still room for improvement in the transparency of companies and social media sites with personal information collected as a means to target ads. There is a connection between trust and transparency; therefore, if businesses clearly state what they are collecting and for which purposes, it could lead to trust-building with consumers, and consumers would potentially, in turn, be willing to provide certain information rather than having it harvested in different ways (Morey, 2015).

Final Thoughts:

The purpose of this research has been to examine the implications of privacy in communication with corporate online data collections practices. I begin in Chapter 1 by traveling through the history of data collection and privacy policy within the United States, gathering a basis of how societal attitude and legislation adapted to the evolution of new technologies. Moving forward, Chapter 2 is an introduction of the internet on a broad scope, followed by more specific actors within the online realm. This particular section gives an increasingly magnified view of how different actors, such as ISPs, edge-providers, and third parties, collect and share information within their capacities. Chapter 3 discusses the online advertising industry and its value in regard to businesses, connecting how the data collected by internet actors are used to target consumers through advertising. Continuing in Chapter 4, I move to discuss general user privacy perceptions and expectations consumers have when online. Privacy and social media are then brought together in Chapter 5 by examination of Facebook and Google's privacy policies to give understanding about opportunities that users are offered to control the information businesses collect. Google and Facebook are used as examples to show the difference between a social media platform/edge-provider and a search engine in privacy and advertising. Following

my examples are my recommendations in which I delineate the need for individual awareness about policies, platforms and privacies, clearly written legislation, and company transparency.

My findings are that consumers, even when expressing concern that companies collect, use, and sell their data, are still largely uninformed about the privacy policies of corporations, nor do people realize the rights they have to their information. This indicates that consumers would benefit from doing their research into the programs and platforms they use. Additionally, the United States lacks legislation surrounding consumer privacy and company policy that would protect consumer information. Furthermore, the United States could benefit from adopting a governing technological privacy policy, as the European Union did in 2018. Finally, corporations such as Google and Facebook have a responsibility to be transparent with their consumers about what they track, collect, and sell, if applicable. Consumers have a right to know how their information is used and dispersed, and they have a right to give or revoke access to their data. My analysis of privacy, data collection, and the actors within the online realm along with a proposal of coinciding recommendations serve as stepping stones that can inspire thought and action in order to create a better and safer internet relationship between users, corporations, and the government.

References

(FOIA), F. of I. A. (n.d.). FOIA.gov (Freedom of Information Act) Learn. Retrieved from https://www.foia.gov/about.html

Allen, R. S., & Scott, P. (1966, June 15). Data Center Plan Called Privacy Invasion. *The Lewiston Daily Sun*, p. 11. Retrieved from https://news.google.com/newspapers?id=ZGogAAAAIBAJ&sjid=3GYFAAAAIBAJ&pg=93 3,5465131&dq=data-center&hl=en

Alhabash, S., Mundel, J., & Hussain, S. A. (2017). Social Media Advertising. Digital Advertising, 285–299. doi: 10.4324/9781315623252-16 Andreou, A., Venkatadri, G., Goga, O., Gummadi, K., Loiseau, P., & Mislove, A. (2018 December 14). Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations1. Retrieved from https://hal.archives-ouvertes.fr/hal-01955309/file/Andreou etal_FacebookAdExplanations_NDSS2018.pdf

Andreou, A., Silva, M., Benevenuto, F., Goga, O., Loiseau, P., & Mislove, A. (2019). Measuring the Facebook Advertising Ecosystem. *Proceedings 2019 Network and Distributed System Security Symposium*. doi: 10.14722/ndss.2019.23280.

About Facebook Ads. (n.d.). Retrieved from https://www.facebook.com/ads/about/?entry_product=ad_preferences

About the FTC. (2020, March 16). Retrieved from https://www.ftc.gov/about-ftc

Andrews, E. (2013, December 18). Who Invented the Internet? Retrieved from https://www.history.com/news/who-invented-the-internet

Baraniuk, C. (2018, October 24). Tim Cook blasts 'weaponisation' of personal data and praises GDPR. Retrieved from https://www.bbc.com/news/technology-45963935

Boerman, S. C., Kruikemeier, S., & Borgesius, F. J. Z. (2017). Online Behavioral Advertising: A Literature Review and Research Agenda. *Journal of Advertising*, 46(3), 363–376. doi: 10.1080/00913367.2017.1339368

Brian Fung, C. T. (2016, October 27). The FCC just passed sweeping new rules to protect your online privacy. Retrieved from https://www.washingtonpost.com/news/theswitch/wp/2016/10/27/the-fcc-just-passed-sweeping-new-rules-to-protect-your-onlineprivacy/

Cahir, J. (2004). The Withering Away of Property: The Rise of the Internet Information Commons. *Oxford Journal of Legal Studies, 24*(4), 619–641. doi: 10.1093/ojls/24.4.619

Cappello, L. (2017). Big Iron and the Small Government: On the History of Data Collection and Privacy in the United States. *Journal of Policy History*, 29(1), 177–196. https://doiorg.washcoll.idm.oclc.org/10.1017/S0898030616000397

Chiu, L. (2013). Drawing the Line Between Competing Interests: Strengthening Online Data Privacy Protection in an Increasingly Networked World. *San Diego International Law Journal*, 14(2), 281–321.

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior,* 101, 1–13. doi: 10.1016/j.chb.2019.07.001

Clement, J. (2019, August 9). U.S. population with a social media profile 2019. Retrieved from https://www.statista.com/statistics/273476/percentage-of-us-population-with-socialnetwork-profile/

Clement, J. (2020, February 18). United States digital population 2020. Retrieved from https://www.statista.com/statistics/1044012/usa-digital-platform-audience/

Cobb, S. (2016). *Data privacy and data protection: Us law and legislation*. ESET. Retrieved from https://www.welivesecurity.com/wp-content/uploads/2018/01/US-data-privacylegislation-white-paper.pdf

Comcast Website Privacy Policy. (2020, January 1). Retrieved from https.//www.xfinity.com/corporate/privacy#section6

Copeland, R., & Needleman, S. E. (2019, November 13). WSJ News Exclusive | Google's 'Project Nightingale' Triggers Federal Inquiry. Retrieved from https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867?mod=hp_lead_pos6

Curac-Dahl, P. (2020, March 17). Third-Party Data: How Does it Fit into Today's Marketing Landscape? Retrieved from https://piwik.pro/blog/third-party-data-fit-today-marketinglandscape/

Custom Audiences Terms. (2019, December 26). Retrieved from https://www.facebook.com/legal/terms/customaudience

Dahlén, M. (2005). The Medium as a Contextual Cue. *Journal of Advertising, 34*(3), 89–98. https://doi.org/10.1080/00913367.2005.10639197

Definition of Edge provider. (n.d.). Retrieved from https://www.lawinsider.com/dictionary/edgeprovider

Dyer v. Northwest Airlines Corporations, 334 F. Supp. 2d 1196 (D.N.D. 2004). (2004, September 8). Retrieved from https://law.justia.com/cases/federal/districtcourts/FSupp2/334/1196/2520672/

El-Abbadi, M. (2019, April 17). Library of Alexandria. Retrieved from https://www.britannica.com/topic/Library-of-Alexandria

Foote, K. D. (2017, September 15). A Brief History of Business Intelligence. Retrieved from https://www.dataversity.net/brief-history-business-intelligence/

Gauthier, J. (n.d.). Data Collection - History - U.S. Census Bureau. Retrieved from https://www.census.gov/history/www/innovations/data_collection/

Google Ads policies - Advertising Policies Help. (n.d.). Retrieved from https://support.google.com/adspolicy/answer/6008942?hl=en

Graham, M. C., & Elias, J. (2020, March 18). Google is still showing mask ads next to coronavirus stories after promising to take them down. Retrieved from https://www.cnbc.com/2020/03/18/google-is-still-showing-mask-ads-next-to-coronavirusstories-after.html

Graham-Harrison, E., & Cadwalladr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-uselection

Horwitz, J., & Seetharaman, D. (2020, March 14). Chenault Leaves Facebook Board After Disagreements With Zuckerberg. Retrieved from https://www.wsj.com/articles/chenaultleaves- facebook-board-after-disagreements-with-zuckerberg- 11584140731?mod=searchresults&page=2&pos=14

How does Facebook show me ads on other apps and websites?: Facebook Help Center. (n.d.). Retrieved from https://www.facebook.com/help/119468292028768?ref=dp

How does Facebook work with data providers?: Facebook Help Center. (n.d.). Retrieved from https://www.facebook.com/help/494750870625830?ref=dp

Instagram Help Center. (n.d.). Retrieved from https://help.instagram.com/477434105621119/?helpref=hc_fnav&bc[0]=Instagram Help&bc[1]=Privacy and Safety Center

IAB. (1n.d.). *Internet advertising revenue report*. Retrieved from https://www.iab.com/wpcontent/uploads/2019/10/IAB-HY19-Internet-Advertising-Revenue-Report.pdf

Internet Hall of Fame. (n.d.). Retrieved from https://www.internethalloffame.org/inductees/timberners-lee

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. doi: 10.1016/j.bushor.2009.09.003

Leicht, K. (2018, November 3). Retrieved from https://blog.jipel.law.nyu.edu/2018/11/post-gdprwill-the-u-s-implement-a-comprehensive-data-privacy-law/

Let's take a look at the full Verizon Privacy Policy. (2020, January 1). Retrieved from https://www.verizon.com/about/privacy/full-privacy-policy#acc-item-31

Litman-navarro, K. (2019, June 12). We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. Retrieved from https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacypolicies. html?searchResultPosition=1

Marr, B. (2015, February 25). A brief history of big data everyone should read. Retrieved from https://www.weforum.org/agenda/2015/02/a-brief-history-of-big-data-everyone-should-read/

Meredith, S. (2018, April 10). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Retrieved from https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-atimeline-of-the-data-hijacking-scandal.html

Morey, T., Forbath, T., & Schoop, A. (2015, May). Customer Data: Designing for Transparency and Trust. Retrieved from https://hbr.org/2015/05/customer-data-designing-for-transparencyand-trust

Nasr, A. (2016, September 27). Roles of FTC, FCC Are Front and Center in Privacy Debate. Retrieved from https://morningconsult.com/2016/09/27/roles-ftc-fcc-front-center-privacydebate/

Namara, M., Wilkinson, D., Caine, K., & Knijnenburg, B. P. (2020). Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 83–102. doi: 10.2478/popets-2020-0006

Nissenbaum, H. F. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books."

Nuñez, M. (2019, November 6). Facebook Is Still Leaking Data More Than One Year After Cambridge Analytica. Retrieved from https://www.forbes.com/sites/mnunez/2019/11/05/facebook-is-still-leaking-data-more-thanone-year-after-cambridge-analytica/#5f6c70b56180

Nurse, J. R. C., & Buckley, O. (2017). *Behind the scenes: a cross-country study into third-party website referencing and the online advertising ecosystem*. Human-centric Computing and Information Sciences. Retrieved from https://link.springer.com/article/10.1186/s13673-017-0121-6

Obar, J. A., & Oeldorf-Hirsch, A. (2016). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2757465

Privacy Policy – Privacy & Terms. (2019, December 19). Retrieved from https://policies.google.com/privacy#footnote-people-online

Raul, A. C. (2019). The privacy, data protection and cybersecurity law review (6th ed.). London, UK: Law Business Research Limited.

Rebecca Moody, R., & Csokasi, M. (2019, December 11). Retrieved from https://digital.com/blog/isp-tracking/

Rouse, M. (2016, November 7). What is clickstream analysis (clickstream analytics)? - Definition from WhatIs.com. Retrieved from https://searchcustomerexperience.techtarget.com/definition/clickstream-analysis-clickstreamanalytics

Rudikowa, L., Myslivec, O., Sobolevsky, S., Nenko, A., & Savenkov, I. (2019). The development of a data collection and analysis system based on social network users' data. *Procedia Computer Science*, 156, 194–203. https://doiorg. washcoll.idm.oclc.org/10.1016/j.procs.2019.08.195

Sir Tim Berners-Lee. (n.d.). Retrieved from https://webfoundation.org/about/sir-tim-berners-lee/

Solove, D. J. (2006). GW Law Faculty Publications & Other Works. Retrieved from https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications

Such, J. M., & Criado, N. (2018). Multiparty privacy in social media. *Communications of the ACM, 61*(8), 74–81. doi: 10.1145/3208039

Taylor, R. (2019, July 26). Facebook and Google Algorithms Are Secret-but Australia Plans to Change That. Retrieved from https://www.wsj.com/articles/facebook-and-google-algorithmsare-secretbut-australia-plans-to-change-that-11564134106?mod=article_inline

Tech Explained: the Glossary. (2018, July 31). Retrieved from https://cdt.org/insights/techexplained-the-glossary/

Tene, O. (2007). What Google Knows: Privacy and Internet Search Engines. *SSRN Electronic Journal*. doi: 10.2139/ssrn.1021490

The Editors of Encyclopaedia Britannica. (2019, April 20). John Graunt. Retrieved from https://www.britannica.com/biography/John-Graunt

The FTC's Endorsement Guides: What People Are Asking. (2019, May 15). Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-whatpeople-are-asking

TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]. (2018, June 28). Retrieved from http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

Top 5 Companies, Ranked by US Net Digital Ad Revenue Share, 2018 & 2019 (% of total digital ad spending). (2019, February 1). Retrieved from https://www.emarketer.com/chart/226372/top-5-companies-ranked-by-us-net-digital-adrevenue-share-2018-2019-of-total-digital-ad-spending

Tracy, R., & McKinnon, J. D. (2019, July 24). Facebook Settlement Requires Mark Zuckerberg to Certify Privacy Protections. Retrieved from

https://www.wsj.com/articles/facebooksettlement-requires-mark-zuckerberg-to-certify-compliance-11563923987?mod=article_inline

U.S. Digital Ad Revenue Climbs to $57.9 Billion in First Half 2019, Up 17% YOY, According to IAB Internet Advertising Revenue Report. (2019, October 21). Retrieved from https://www.iab.com/news/u-s-digital-ad-revenue-climbs-to-57-9-billion-in-first-half-2019/

U.S. FTC. Protecting childrens privacy under COPPA: a survey of compliance, Protecting hildrens privacy under COPPA: a survey of compliance (2002). Washington, DC.

U.S. Govt. Print. Office. Records, computers and the rights of citizens: report, Records, computers and the rights of citizens: report (1973). Washington, D.C.

Urton-Washington, J. (2016, August 19). More third parties know what you do online. Retrieved from https://www.futurity.org/third-party-web-tracking-1230222-2/

Voorveld, M., van Noort, G., Muntinga, G., & Bronner, F. (n.d.). Engagement with Social Media and Social Media Advertising: The Differentiating Role of Platform Type. *Journal of Advertising, 47*(1), 38–54. https://doi.org/10.1080/00913367.2017.1405754

What We Do. (2017, July 10). Retrieved from https://www.fcc.gov/about-fcc/what-we-do

Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y., & Chen, Z. (2009). How much can Behavioral Targeting Help Online Advertising? Retrieved from http://www2009.eprints.org/27/1/p261.pdf

Zurbriggen, E. L., Hagai, E. B., & Leon, G. (2016). Negotiating privacy and intimacy on social media: Review and recommendations. *Translational Issues in Psychological Science*, *2*(3),248–260. doi: 10.1037/tps0000078