Surveillance Capitalism and the Right to Be Forgotten: Does the General Data Protection Regulation or the California Consumer Privacy Act Better Protect Individual's Data Privacy in a Surveillance Economy?

Surveillance Capitalism and the Right to Be Forgotten:

Does the General Data Protection Regulation or the California Consumer Privacy Act Better Protect Individual's Data Privacy in a Surveillance Economy?

Jasmin Frankel

A Thesis in the Field of International Relations

for the Degree of Master of Liberal Arts in Extension Studies

Harvard University

November 2021

Abstract

The Western economy flourishes because of its capitalistic system, a system that is solely dependent on the success of commerce. The development of the internet, the evolution of technology and the integration of both resulted in a transformation of the capitalistic business model. Companies can now predict and influence consumer purchases by collecting and analyzing consumer data, thus ensuring profitability and guaranteeing the success of businesses with the goal of better service. However, does this model best serve consumers?

Scholar Shoshana Zuboff exposes many concerns over data collecting business practices, or what she describes as surveillance capitalism. Consumers' habits are continuously monitored, often without their knowledge or proper consent, leaving little room for privacy. Online businesses, not governments, have been left to self-regulate consumer practices, but as concerns grow, governing bodies are beginning to enact data privacy regulations. In 2018 the European Union passed the General Data Privacy Protection (GDPR), and in 2020 the state of California (in the United States) passed California Consumer Privacy Act (CCPA) to protect the data privacy rights of individuals when using online services.

This thesis aims to determine if the GDPR or the CCPA is better equipped at addressing data privacy violations discussed by Zuboff. The Zuboff Rubric - two scales developed for this thesis based on her observations of asymmetries of knowledge and power and the absence of legitimate detection and sanctions - is used to determine each law's ability.

The results of the Zuboff Rubric reveal that the GDPR and the CCPA have many similarities in providing certain aspects of data privacy protections, such as an individual's right to request data deletion from a business' database and to be provided information by businesses on the functions of the data processed. However, there are many aspects of data protection not covered by the CCPA but are covered by the GDPR, proving that the GDPR is better equipped to protect consumer data privacy and provide consumers more control over their data.

Author's Biographical Sketch

Jasmin Frankel is a graduate student at the Harvard Extension School focusing on international relations. She has her B.A. in journalism and political science from SUNY Stony Brook University. Upon graduating, she was a reporter and an actress. She recently owned her own business, a movie theater, but was forced to shut down operations permanently due to the Covid-19 global pandemic. Out of all her professional endeavors, academia is by far her most passioned one. "Life is for learning. This thesis has undoubtably taught me many valuable lessons."

Jasmin most recently was a Deputy Campaign Manager for a City Council candidate in Queens, NY, where she learned a lot about local policy. She hopes to go to law school next to focus on data privacy law - as this thesis discusses, laws surrounding individuals' data privacy are much-needed for our internet-dependent lifestyle. As a millennial, Jasmin is fortunate enough to have known a society without all the complications of the internet but appreciates the ability to access the world at her fingertips. She has two kitties - June and Jane - and a collection of plants, which became a new, much-loved hobby during the pandemic.

Dedication

I would like to dedicate this thesis to all those, young and old, who do not understand the inner workings of the internet and to Shoshana Zuboff for writing about surveillance capitalism. She has helped me understand that the feeling of "something wrong" when online companies request personal information is in fact an appropriate reaction and that there has not been anything wrong with my gut feeling. Instead, there is actually something wrong with the business model that is commonly presented to us paired with unfortunate desensitization of privacy violations within society. These pressures still exist today in professional and personal settings but are slowly getting better with knowledge and awareness.

Acknowledgements

I would like to thank my mom and dad for their support during this rigorous thesis process. I want to thank Ramel Racelis, Terrill Lim, Divine Gordon and Leah Pagnozzi for spending many hours talking to me about this thesis. I would like to give a special thanks to Misan Oteri, who has been somewhat of a mentor to me during my time at HES and helped motivate me through this writing process. I also would like to thank Madeleine Goodman for stepping in last minute to me help review my grammar. I am also grateful for discovering Naruto while writing this thesis, for it has helped during my much-needed mini brakes and provided me with inspiration to keep working hard. I want to thank Dr. Doug Bond for telling me that I should follow my heart and pick a topic I would be passionate about; the topic was there all along. I would also like to give a huge thank you to Dr. Ariane Liazos, who spent (I am sure) a grueling year helping me to develop this piece of work. I am proud of this thesis and am thankful to have had all of these wonderful people there to support me.

Table of Contents

List of Tables

Chapter I.

Literature Review of Scholarship on Big Data and Surveillance Capitalism

Technology is a useful servant but a dangerous master.

- Historian Christian Lous Lange, Nobel Lecture, 1921[1]

When was the last time you spent a day without any digital devices? Could you imagine not logging into social media, ordering food with a few clicks or asking your digital assistant to play music while providing new restaurant recommendations? Many societies have become heavily dependent on the services provided by internet-based technology, but have you ever thought about what goes on behind the scenes of your inquiries and requests?

As it turns out, all your activity is monitored, recorded, compiled and analyzed to better serve you. You may have already learned technology collects activity data. You may even find it convenient, but do you know how much and what type of data is collected in the process? Is the data collection based on your desires or maybe your thoughts or your behaviors or maybe the way your eyes move during a Zoom call? Technology now knows more about us as individuals than most of us know about ourselves. Is this something we even wanted?

Technological innovations have forced an evolution in capitalism. The release of the internet and its initial failure of the dotcom bust led to the development of a business

---

[1] Christian Lange, "Noble Lecture," (December 13, 1921), NobelPrize.org, https://www.nobelprize.org/prizes/peace/1921/lange/lecture/.

model that ensures online sales. As online companies were already collecting user data, analysts began reviewing the data to determine user habits to guarantee sale success. This form of consumer surveilling has turned traditional capitalism into what Scholar Shoshana Zuboff calls surveillance capitalism.[2]

Data collection and analyzation of human habits are not new devices employed by capitalism, but technology has permitted a new level of invasiveness. As more of our daily routines revolve around internet-based technology, our lives are put on display, providing accessible insight into our behaviors for the world to watch and prey upon. Many scholars have significant concerns over the data harvesting business model, while others believe data aggregation will improve the lives of many.

The European Union (EU) and several state governments within the United States (US) are attempting to address these concerns over the ever-evolving surveillance capitalism economy by providing data privacy protections to the individual. This thesis aims to determine if the European Union's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) is better equipped to regulate businesses' collection of data, while offering individuals control over the information they choose to keep private.

Review of Literature

This review of literature elaborates on the research of data privacy and the tug of war between businesses' collection of data in exchange for free and convenient services

---

[2] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (2015): 75-89, https://journals.sagepub.com/doi/10.1057/jit.2015.5.

and consumers' right to privacy and control of personal data. Some economists argue that data aggregation benefits those who want the convenience of technology to assist with day-to-day tasks. Opposing scholars argue that data aggregation is a disadvantage for consumer privacy, as businesses often perform invasive around-the-clock surveillance of consumers without their acknowledged permission.

Benefits of Data Aggregation

The internet can seamlessly connect almost every aspect of our lives and, by doing so, can offer a unique and personalized experience. This experience is only made possible by the collection and analyzation of user data. Chief Economist at Google, also advisor to Kaggle and Premise (Google backed companies), Hal R. Varian offers insight in his article "Beyond Big Data" on the benefits of big data and why this model is here to stay.[3]

After extensive observation, Varian shares that computer-mediated transactions continuously provide benefits for individuals and businesses. All online actions that consumers perform is an opportunity for computers to collect individuals' data and creates an atmosphere for consumers to receive uniquely tailored experiences. This method allows businesses to provide consumers with what they need quickly and accurately with little effort from the user.[4]

---

[3] Hal R. Varian, "Beyond Big Data," *Business Economics* 49 (2014): 27-31, https://link.springer.com/article/10.1057%2Fbe.2014.1.

[4] Varian, "Beyond Big Data," 27.

He argues that the personalized experience is beneficial for everyone — businesses and consumers. His argument is supported with the evidence that businesses improve by predicting the consumers' needs and desires. The individualized approach leads to more guaranteed sales which saves businesses time, effort and capital. Companies no longer need to curate randomized consumer target lists, which does not guarantee effective sales. Data aggregation and analyzation have significantly improved economic performance and provided innovative capabilities for new types of transactions. He argues that the personalized experience is beneficial for everyone.[5]

The uses and benefits of data aggregation is broken down into four categories: data extraction and analysis, personalization and customization, continuous experiments and new contractual forms due to better monitoring. These techniques significantly improve economic performance while providing innovative capabilities for new types of transactions for consumers. It is expected that an increasing number of businesses will utilize at least one or more of these techniques as a method of improving sales.[6]

Furthermore, he asserts that the first crucial step to data extraction and analysis is to have a physical location to store data. Companies can receive trillions of pieces of data from users every few seconds. If that data cannot be stored, then it cannot be analyzed. Tech giants solved this problem by developing data storage facilities. Since then, the technology-based economy has been significant for businesses to analyze consumer sale habit because predicting behavior is crucial for business growth.[7] Amazon, Google and

[5] Varian, "Beyond Big Data," 28.

[6] Varian, "Beyond Big Data," 27-31.

[7] Varian, "Beyond Big Data," 28.

Netflix are common examples of companies that cater to users needs or desires based on recent purchases, locations or searches, thereby, revolutionizing the market with these abilities.[8]

Through observation of consumer behavior, the streaming company Netflix became aware that 75 percent of movie views occurred because of recommendations of other users. This revelation led Netflix to create a competition to find a machine learning algorithm that would figure out user preferences and then offer movie recommendations themselves. The competition led to the development of Kaggle, an online community of data scientists and machine learning practitioners which now hosts data based projects to make predictions for various-sized companies. Enabled with the capability of running a precisely detailed statistical analysis on user data, companies are seeing profits significantly increase unlike never before.[9]

Varian continues with the point that it is not just businesses benefiting from data collection but also consumers. Consumers are receiving technology-based services fitted to their lifestyle. Some may have concerns over the continuous tracking and monitoring of their behaviors as it requires an excessive amount of information, but Varian assures his readers not to worry. The information provided by consumers allows for mutually beneficial, detail-oriented services to exist, just as doctors, lawyers, accountants, and many other professionals, who collect information to provide their clients with the services needed.[10]

---

[8] Varian, "Beyond Big Data," 29.

[9] Varian, "Beyond Big Data," 28.

[10] Varian, "Beyond Big Data," 28.

Varian believes that despite current fears of such technology, there will always be a desire for technological advancements because of its ability to bring luxury and convenience to users. One example where consumers are utilizing the convenience of data-driven technology is with the use of digital assistants. Employed as a home accessory, digital assistants can play users' favorite music, remind users of meetings, predict the local weather and so much more. For digital assistants to provide such requests in granular detail, they must know users intimately. The more information devices can collect from their users, the more accurately they can provide services.[11]

However, Varian points out that gathering information is not enough. After collection, data needs to be put through an experimentation process to guarantee the production of the desired outcome. A company like Google runs roughly 10,000 experiments a year on their users, many of which are performed through searches from their free search engine and advertisement clicks. Experiments provide a way to understand demand function. In fact, Varian reflects on Larry Page's comment about Google: "It should know what you want and tell it to you before you ask the question," noting that this desire has now become a reality.[12]

Varian states that an increasing number of various-sized companies are using data collection and behavior predicting algorithms to serve consumers better and improve business sales. By creating an information atmosphere, businesses no longer need to guess what consumers want to purchase; instead, companies can directly send targeted

---

[11] Varian, "Beyond Big Data," 28.

[12] Varian, "Beyond Big Data," 28-29.

ads to potential consumers and save on high advertising costs. Even the richest man in the world, Jeff Bezos, creator of Amazon, is not immune to enjoying a personalized experience. When signing on to his Amazon account, Bezos received a message based on his purchase history suggesting that he reads the *New York Times*, *Chicago Tribune* and *Los Angeles Times*.[13]

Varian concludes that not only has data collection and experimentation become a vital asset to business growth, but consumers have also grown accustomed to having personalized experiences. With all the conveniences of technology, he provides a complete overview of how companies can utilize data and technology to improve the consumer experience.[14]

The importance of personalization and the consumer experience during an online transaction is also reflected in the article "Big Data: The Management Revolution." Economists Andrew McAfee and Erik Brynjolfsson argue that businesses can serve their consumers better while increasing profit margins by obtaining big data. McAfee and Bryniolfsson consider big data "a management revolution," which easily allows online companies like Amazon to put brick-and-mortar stores out of business.[15] Online stores can do something traditional stores could not before - rely on large amounts of factual data instead of making decisions based on gut and intuition.[16]

---

[13] Varian, "Beyond Big Data," 28.

[14] Varian, "Beyond Big Data," 27-31.

[15] Andrew McAfee and Erik Brynjolfsson, "Big Data: The Management Revolution," *Harvard Business Review*, (October 8, 2014): 1-9, https://hbr.org/2012/10/big-data-the-management-revolution.

[16] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 4.

McAfee and Brynjolfsson present three reasons big data is significant to business success: volume, velocity and variety. The amount of data created each day has reached astronomical numbers and continues to grow. For example, in 2012, the amount of user data created each day averaged 2.5 exabytes.[17] They write, "Each of us is now a walking data generator."[18] Companies can now gather data from a wide variety of resources that connect online. Such a variety provides information on every topic imaginable, at a much lower cost. The second significant variable in which data-based businesses need to utilize for consumer success is the speed at which data is collected. Information collected up to the very second can provide immediate insight into consumers' behavior, allowing businesses to alter accordingly.[19]

They lead a team at MIT Center for Digital Business in partnership with McKinsey's business technology office to prove that collecting consumer data provides considerable benefits to businesses. They invited Lorin Hitt, a Wharton colleague, and Heekyung Kim, an MIT doctoral student, to help conduct interviews and gather data from 330 public North American companies. The interviews helped determine the success and failures of businesses that aggregated data versus those that did not aggregate data to make business decisions. The study determined that companies using big data performed better operationally and financially. Some companies have even used big data to sell more products and create new businesses, proving that big data helps improve economic

---

[17] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 4.

[18] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 5.

[19] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 5.

ventures.[20] Among the companies the team met with and interviewed, McAfee and Brynjolfsson discuss two significant examples of highly successful data-driven businesses that decided to shift processes resulting with millions in profits: an airline company and a nationwide big-box chain.[21]

McAfee and Brynjolfsson note that when a big US airline company began using PASSUR Aerospace, an aviation decision-support company that predicts arrival times of aircrafts, the costs associated with flight time miscalculation decreased significantly. Before implementing PASSUR Aerospace's RightETA technology, arrival times were determined by the pilot's estimation. However, unpredictable factors can interfere with arrival times, leaving crew and passengers waiting for a plane to arrive or rushing to accommodate an early arrival flight. PASSUR can provide information on flight factors such as a change in weather conditions or nearby aircrafts en route by aggregating data from the plane and its passengers. This technology determines the real-time location of an aircraft, saving airline companies several millions of dollars.[22]

Furthermore, another example McAfee and Brynjolfsson provide in how data supports economic growth is by utilizing data at a more concentrated level. Sears Holdings, which comprises of Sears, Craftsman and Lands' End brands, determined that by utilizing the data they had on their customers in more specific ways, the company could better target and promote products. The company discovered that each store location has distinct clientele and, therefore, particular needs. Before narrowing down the

[20] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 6.

[21] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 6-7.

[22] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 6.

data, which resulted in increased sales, Sears Holdings would gather data on all their stores nationwide and make decisions on promotional items based on those broad findings. This process took weeks and did not stimulate nationwide sales effectively, but by focusing on clusters of information that could be collected and analyzed on a smaller scale, the company is now able to target popular items by location. This observation and redirection of data concentration sped up the processing time for analyzing data while developing location-based item promotions suitable for consumer needs in the area, allowing for improved advertisement targeting to draw in more customers and increase profits while decreasing expenditures.[23]

Although data provided these businesses with considerable success, McAfee and Brynjolfsson also emphasize the importance of consulting business experts. They are often the ones who ask the questions that need observing. Data is simply the driving tool in providing highly accurate information to answer the critical questions asked by experts and assist in decision-making. Similar to Varian's observation on the use of big data, they found that a company can have a high success rate by basing operational decisions on consumer habits (i.e., if a company starts with the right question, manipulates data to determine the potential outcomes and tailors operational practices based on observations). Additionally, these researchers, like Varian, address concerns over data privacy as the trend of data aggregation and experimentation expand within businesses, but they insist

[23] McAfee and Brynjolfsson, Big Data: The Management Revolution," 7.

that data-driven decisions are by far the best solution for both businesses and the consumers they serve.[24]

These two articles provide insight into how data aggregation can successfully benefit businesses and their consumers. These real-life examples prove how wildly successful businesses can become by simply looking at data. They also prove that consumers can benefit from a customized user experience. Utilizing data aggregation tools is no different from collecting surveys to identify best practices. Compared to survey responses that only willing participants provide, data aggregation allows for a more precise insight into consumer habits, albeit often without consumer consent, and is much more cost-effective.

Many economists praise the development of this technological advancement, but do consumers understand what goes into developing a uniquely-tailored user experience? If they did, would they still be open to having their data collected? Several scholars find the process of data collection to be a violation of consumer privacy rights. Here are some disadvantages of data collection.

Disadvantages of Data Aggregation

Although Varian and McAfee and Brynjolfsson are just three examples of scholars who discuss how data collection can benefit sale accuracy and offer better services. The opposing side, however, expresses concerns over data aggregation or what some call data harvesting. At the forefront of this conversation is Shoshanna Zuboff,

---

[24] McAfee and Brynjolfsson, "Big Data: The Management Revolution," 9.

professor emeritus of the Harvard Business School, who has studied and documented her concerns with data harvesting since the 1980s. She coined the concept surveillance capitalism to describe how businesses follow consumer habits to sell products. In her article "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Zuboff addresses major concerns over Varian's article "Beyond Big Data," where she describes the secrecy of data collection and its use as a tool to manipulate the human psyche. Companies have found a way to blur the lines of business and personal life where invasiveness is almost invisible. The surveillance capitalism business model is to "predict and modify human behavior as a means to produce revenue and market control."[25]

Zuboff focuses on Google as a prime example of how capitalism has invisibly invaded our most intimate areas of life. The article begins with some alarming details of Google's business model.[26] (Such details may be limited due to the lack of legally required transparency with consumers and the heavily guarded technology-based operational labor.) In 2009, Google's Chairperson Eric Schmidt publicly stated in an interview that the search engine not only collects information but stores it for an undisclosed period and commonly shares it with authorities. This comment became a revelation to many consumers.[27]

Google continuously pursues ways to extract data from users, which Zuboff describes as a one-way relationship that permits a void of dialogue and consent. By

---

[25] Zuboff, "Big Other," 75.

[26] Zuboff, "Big Other," 75.

[27] Zuboff, "Big Other," 75.

listing the many methods Google unsuspectingly penetrates devices to obtain data (e.g., via voice communication or bypassing privacy settings), she emphasizes that these practices raise significant concerns since many users are unaware of these methods even occurring. The biggest hurdle we face in society, according to Zuboff, is the lack of transparency of the corporate data-harvesting business model. Without such information, individuals are unaware of how they are being manipulated. It then becomes impossible for individuals to fight for their privacy rights without this proper knowledge.[28]

Many data collecting sources exist, such as computer-mediated transactions, Internet of Things, corporate and government databases and, lastly, publicly accessible data (i.e., satellites, Google Street View, Wifi networks). The means by which this data is collected are questionable as exemplified by the development of Google Street View. In a lawsuit filed by the Attorneys General from 38 states and the District of Columbia for Google practices, according to an Electronic Privacy Information Center's (EPIC) report, Google was found to have engaged in unauthorized collection of data. Google was permitted to settle the case for seven million dollars and keep the Street View images collected, which are globally utilized today.[29]

Data extraction is a forced social acceptance by the ever-growing business model of surveillance capitalism, according to Zuboff. Users are drawn to free products but are unaware of what they pay in exchange for accessing such products. Although Google prides itself on providing high-quality services, which are made possible through data

---

[28] Zuboff, "Big Other," 82-83.

[29] Zuboff, "Big Other," 79.

analyzation, she notes that such practices result in power asymmetries. Additionally, the lack of transparency in how consumers' data is processed and the lack of knowledge of it even being collected leaves little room for privacy self-management. "Google knows far more about its populations than they know about themselves."[30]

Zuboff's statement, "we have not yet successfully defined 'big data' because we continue to view it as a technological object, effect or capability"[31] serves to strengthen this argument that consumers largely do not understand the processes that take place when they interact with the internet. This realization also shows how little regard companies have for their users' privacy preferences in return. Zuboff, however, does acknowledge that computer transactions have brought innovation and transparency to society in a way unlike ever before and will undoubtedly remain to do so for the foreseeable future.[32]

Zuboff is not the only one who is concerned with the accessibility businesses have to consumers' data. Philosopher Helen Nissenbaum of the Information Science Department at Cornell University pushes the idea of further regulations when dealing with online privacy in her article "A Contextual Approach to Privacy Online." She writes that the average person does not understand internet jargon or how it functions, which

---

[30] Zuboff, "Big Other," 75.

[31] Zuboff, "Big Other," 78.

[32] Zuboff, "Big Other," 78.

leaves users susceptible to data collection and control. The best way to combat such vulnerabilities is by holding online businesses accountable.[33]

According to Nissenbaum, "We should not expect social norms, including informational norms, simply to melt away with the change of medium to digital electronic any more than from sound waves to light particles."[34] Many companies including Google have promised to commit to an invisible barrier, which would keep identifiable records of their users private. However, it is difficult to identify Google's efficacy in fulfilling such practices because we do not have access to their business operations. The mechanisms for user privacy protections such as company privacy policies and notice-and-consent options have been put into place but there are many flaws within these practices.[35]

Privacy policies are often long and filled with legal jargon which everyday users may not comprehend. Additionally, users must actively search for the corresponding policy of a service to learn if it is in effect, which can abruptly change as businesses have the right to update or modify their policies at any given time. Consumers also have the burden of searching for the notice-and-consent option where they can choose to opt-out of data collection. Although, even when choosing to opt-out, users are still unaware of the

---

[33] Helen Nissenbaum, "A Contextual Approach to Privacy Online," *Daedalus* 140, no. 4 (Fall 2011): 30-48, https://www.amacad.org/sites/default/files/daedalus/downloads/Fa2011_Protecting-the-Internet-as-Public-Commons.pdf.

[34] Nissenbaum, "A Contextual Approach to Privacy Online," 43.

[35] Nissenbaum, "A Contextual Approach to Privacy Online," 43.

level of actual control they have over their data. The opt-out alternative provided to consumers is still a weak representation of choice.[36]

It is still unclear to what extent notice-and-consent protects user privacy choices when it comes to data. Due to the internet's complexities, it would take a team of experts to follow the path of all online interactions to determine if they are protected or not. Nissenbaum does call for "brief and clear policies" in which businesses provide short and easy-to-read user policies, giving more control back to consumers. This type of policy would require businesses to be transparent.[37]

The internet mainly evolves around for-profit entities, with a few public service government websites, making it predominately privately operated. Therefore, if the online world is a for-profit, commercially-driven marketplace, federal agencies like the Commerce Department and the Federal Trade Commission should oversee online transactions as they do with in-person transactions. Although Nissenbaum supports this ideology over online businesses, she notes its difficulties as many companies veil their desire to profit from their online traffic. For example, Google, when first launching, shunned advertisers and provided free services to users. With its parent company worth $1 trillion in market value as of 2020,[38] Google now heavily relies on advertisements as

---

[36] Nissenbaum, "A Contextual Approach to Privacy Online," 34-35.

[37] Nissenbaum, "A Contextual Approach to Privacy Online," 36.

[38] Sergei Klebnikov, "Google Parent Alphabet Passes $1 Trillion in Market Value," *Forbes*, (January 13, 2020), https://www.forbes.com/sites/sergeiklebnikov/2020/01/13/google-parent-alphabet-set-to-hit-1-trillion-in-market-value/?sh=190b55a14dcf.

its primary business model. This example is just one of many on how online companies portray one desire but then utilize their abilities to profit off unsuspecting users.[39]

There is a lack of creative evolution in protecting individuals' privacy rights. As the complex infrastructure of the internet transforms, so do users' vulnerabilities. Nissenbaum calls for specific actions to be viewed as confidential, as the same actions would be considered private and safeguarded during in-person transactions. There should be an expectation of privacy provided to users. If a company decides that data aggregation is the only way to profit, those practices should be explicitly shared with consumers. This information offers consumers the decision to determine if they would like to partake in the transaction. Consumers should have the ability to possess control over their data with business practice transparency and opt-out capabilities.[40]

Over the years, as the internet expanded globally, there have been many missed opportunities to legally regulate online businesses. Communications scholar Sarah Myers West examines the early origins of what she refers to as the data capitalism business model in her article "Data Capitalism: Redefining the Logics of Surveillance and Privacy." In the article, West details the very early origins of data collection to increase sales and provide insight into the gap of consumer legal protections. Data capitalism can be traced back to the late 17th century when censuses were often taken in England to understand social problems and during the same period were also used by Westerners who collected statistical information to understand Southeast Asian cultures to attempt to

---

[39] Nissenbaum, "A Contextual Approach to Privacy Online," 41-42.

[40] Nissenbaum, "A Contextual Approach to Privacy Online," 44.

gain social control. Data collection does look quite different today with the evolution of technology, which has turned into common online business practice. This business practice did not stem from the development of the internet but has exponentially increased its usefulness because of the online intermediary.[41]

With the release of the World Wide Web in homes, companies were eager for the internet to gain traction globally. Businesses began inflating their value, leading to the dotcom market crash. After the crash, companies were left scrambling to cultivate a profitable business model quickly. To entice consumers back online, Silicon Valley entrepreneurs began offering free online services. Several companies, including Amazon and IMB, figured out that user data could be the answer. By running experiments, companies discovered cookies which are "text files with small pieces of data" that can remember facts about the activities of its users, providing an effortlessly individualized experience.[42] This method drew consumers back to the internet, but businesses needed to figure out how to profit from their new traffic.[43]

West argues that the development of the cookies technology fostered a whole new online world. Cookies track users' behavior and store that information for it to be analyzed and experimented on to determine consumers' needs and desires. That

---

[41] Sarah Meyers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy," *Business and Society* 58, no. 1 (2019): 20-41, https://journals.sagepub.com/doi/10.1177/0007650317718185.

[42] Ken Colburn, "Computer cookies: What they are and how to manage them," Microsoft News, (October 19, 2020), https://www.msn.com/en-us/news/technology/computer-cookies-what-they-are-and-how-to-manage-them/ar-BB1aaQWH.

[43] West, "Data Capitalism," 25-27.

information can then be utilized to create a profile of each consumer who can now be targeted with specific ads and information. West writes:

> …the use of cookies to track users' activities across the web are not used solely by Internet companies—financial companies, credit rating associations, political parties, and others use many of these technologies—it is the Internet companies, the technology makers, who have most contributed to an information environment in which every action, digitally and increasingly in real life, leaves behind traces that are collected by companies for commercial purposes.[44]

The media praised cookie technologies for their ability to accumulate information. However, West maintains that this was a golden opportunity for US governing bodies to ensure legal protections for consumers. Instead, the US Department of Commerce created a framework that left companies in charge of making decisions regarding how to handle users' data. This decision was pivotal in how online businesses operate with consumers. Meanwhile, the EU met much more success in restricting data with the onset of the internet by implementing the Data Protective Directive, which has been succeeded by several laws that further protected data privacy.[45]

One additional concern in the business of data aggregation is data brokers. Third-party companies, or data brokers, buy aggregated consumer data from businesses and utilize it to sell targeted advertisements. This forces users to actively protect their data, which many cannot do due to the lack of cookies technology awareness or the proper mechanisms to prevent data collection.[46]

---

[44] West, "Data Capitalism," 21.

[45] West, "Data Capitalism," 28-29.

[46] West, "Data Capitalism," 30-31.

Users can attempt to protect their data by deleting their web histories, which partially protect some elements of the user's data but not most. Advertising companies eventually became aware of this method and then pushed for more aggressive browser tracking. The development of the Web beacon soon replaced cookies to continue monitoring every online move, from images to microphones and even mouse movement.[47]

One company that assisted with the evolution of innovative tracking technology is Google. Similar to Zuboff, West presents concerns over Google's business practices. West's focus is different, however. She explores the advertising aspect of the Google platform. After the dotcom bust, Google was one of the pillar companies to figure out that by utilizing the data from the searches on their search engine, the company could target advertisements to specific consumers who would find them helpful. This discovery led to Google developing code that installs itself into users' computers every time an ad is clicked. With the acquisition of DoubleClick, a cookie technology company, Google's ability to intensely observe consumers magnified. Armed with the evolution of cookies, Google can garner a never-ending stream of data while providing users an abundance of monetarily free services in return.[48]

Economists Varian and McAfee and Brynjolfsson present strong arguments for the future of data collection and how it has helped consumers. Contrarily, scholars Zuboff, Nissenbaum and West show how this process, in many ways, violates consumers.

---

[47] West, "Data Capitalism," 30.

[48] West, "Data Capitalism," 32.

However, data collection and experimentation will not be going away any time soon as surveillance capitalism is the new capitalistic business model that is now ingrained in our society. The next and perhaps most important step is to create and implement rules and regulations that protect everyone who uses devices connected to the internet. Without regulations, consumers will be faced with vulnerabilities unforeseen by today's society. Therefore, how can governments better regulate data aggregation to maintain the economic benefits while addressing privacy concerns?

Chapter II.

Literature Review of Scholarship on Cultural Norms and Legal Precedents Regarding Privacy in the United States and Europe

Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

- Edward Snowden[49]

---

[49] Paul Schrodt, "Edward Snowden Just Made an Impassioned Argument for Why Privacy Is the Most Important Right," *Business Insider*, (September 15, 2016), https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9?op=1.

Zuboff, Varian and others have made it apparent that data collection is both desired and feared. Too much data and businesses become overly invasive into our personal lives. Not enough data and computer-mediated technology will not be able to perform at its peak level of service. One thing that is certain: both businesses and consumers heavily depend on online technology. The question then becomes "How can governments step in and effectively regulate data privacy?" The EU and the US are societies with laws that support privacy, but those rights take different forms as societal beliefs regarding privacy vary.

Legal scholar James Q. Whitman writes about differences in societal norms and legal precedence surrounding privacy in the US and EU. In his article "The Two Western Cultures of Privacy: Dignity Versus Liberty," Whitman prefaces the two Western views by writing that privacy is often sought after as it is considered a universal right. Although privacy is revered by most, it is complicated to define. Privacy conforms not only to cultural beliefs but also changes over time as cultural beliefs face modification. When providing details on the evolution of privacy within several countries, Whitman reiterates that privacy cannot be determined from logic but through experience and necessity.[50]

Whitman lists the development of various privacy beliefs throughout the decades and notes that although the two governing bodies hold the same Western beliefs, they have very different definitions of privacy. For example, the EU and the US do not agree on how privacy is handled in situations pertaining to public figures, invasion of one's home, nudity, and the media. The Europeans' desire is to maintain privacy from

---

[50] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," *Yale Law Journal* 113, no 6 (April 2004): 1153-1251.

neighbors while Americans' desire to maintain privacy from the government. In Europe, protecting individuals' images prevents public indecency, shame and humiliation. In contrast, Americans are more concerned with government interference of one's home or communications. Freedom of speech holds high value in the US, even if it exposes information within one's personal life. This apparent difference helps provide a better understanding of the decisions made by these two governing societies and the legal regulations by which they abide.[51]

Most Americans desire liberty and honor from political suppression and are almost always often suspicious of the State, considering it the prime enemy of individual privacy. Several case rulings prevent government intervention in personal decisions, such as *Roe v. Wade*, which guarantees the right to an abortion and keeps it private. Support for privacy rights continues with the ruling of *Whalen v. Roe*, which involved the government collecting private information. The case *Schmerber v. California* described the Fourth Amendment to protect privacy against the State. Thus, when it comes to privacy in the US, one belief remains: Americans view their homes as the primary defense and the State as the primary enemy.[52]

The historical development of European privacy laws are often approached with consideration on how businesses maintain profitability while respecting the individuals' privacy. For example, the origin of privacy laws in France dates back to the Constitution of 1791, which incidentally also provided extensive freedom to the press. Between the

---

[51] Whitman, "Two Western Cultures of Privacy," 1211-1212.

[52] Whitman, "Two Western Cultures of Privacy," 1215-1216.

1820s and 1840s, there were increasingly little protections for one's private life as a new law lifting press censorship passed in 1819. This period marked growing support for freedom of the press, further limiting individuals' privacy. However, the view of free speech partially changed in 1867 when Alexandre Dumas père had an indecent photograph taken of him without his permission. Dumas sued the photographer, and the court ruled that the person in the image has ownership over the picture, not the person who took the picture. The social and legal mindset resulting from this ruling has helped create the framework that shaped France's view of privacy.[53]

The concept of image ownership belonging to the subject of the photo extends throughout the EU, regardless of the person being a public figure or not. Additionally, if an indecent picture is published, a website host is held accountable and faces liabilities. Conversely, subjects do not assume ownership of their photographic image nor have control over the image in the US despite indecency of the photo or public distinction. American courts commonly believe that once a photo is published online, it becomes too late for recovery, and therefore, the situation is not rectifiable.[54]

These examples of opposing privacy beliefs within the EU and US exemplify that privacy is a complicated issue worldwide. It can be seen that Americans and Europeans distrust each other's laws regarding privacy because of such contrasting views, although subtle legal similarities do exist. Whitman also notes that societal norms are not an absolute characterization of all residents. However, privacy is a significant right in the

---

[53] Whitman, "Two Western Cultures of Privacy," 1171-1179.

[54] Whitman, "Two Western Cultures of Privacy," 1198-1199.

EU and the US, and its meaning varies as privacy laws stem from historical events and legal decisions that shape countries practices.[55]

Legal Scholar Paul M. Schwartz adds to the discussion of differences in data privacy regulations in the EU and the US in his article, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures." Schwartz notes that the EU has played an influential role in international decisions regarding information privacy since the 1990s. The push for information privacy began on the state level in 1970 when the Hessian Parliament enacted a privacy statute in Germany. Other countries soon followed suit. The statute led to enacting the Fair Information Practices (FIPs), which define core obligations for public and private sectors that process personal data. Throughout the 1980s, the Council's Data Protection Convention developed essential European-wide agreements regarding data privacy.[56]

Since privacy is recognized as a human right in the EU, one primary focus for developing data privacy regulations is to prevent the violation of that right. Debates about the potential of human rights violations versus the limitations on the free flow of data across frontiers are not uncommon. However, the EU's objective is to find a middle ground solution.[57]

---

[55] Whitman, "Two Western Cultures of Privacy," 1153-1251.

[56] Paul M. Schwartz, "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures," *Harvard Law Review* 126, no. 7 (May 2013): 1966-2009, https://harvardlawreview.org/2013/05/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/.

[57] Schwartz, "The EU-U.S. Privacy Collision," 1977.

Data privacy laws do not just protect residents' data within the EU borders but also aim to protect residents' data when transferred abroad. Data from the EU can only be transferred to third-party countries if they have proper protocols for protecting data. This regulation is highly regarded and allows for only limited exceptions. EU privacy regulations have proven to be influential not just within the EU but globally.[58]

The EU has effective government regulators to enforce its standards globally, although many countries already respect the data protection standards, especially when trading with the EU Member States. The EU is considered non-divisible, meaning there is one set of standard expectations for all economies with which they do business. However, there are exceptions for the US. The EU and the US have entered into many trade agreements such as the Safe Harbor Program, Model Contractual Clauses, and Binding Corporate Rules, which overlook the traditional regulatory data expectation imposed on most countries. However, the agreements are meant to set compliance benchmarks for the US when handling data of EU residents.[59]

Schwartz calls the US the great exception due to the country's lack of federal data privacy laws. Instead, the US regulates privacy on a sector basis. For example, the Health Information (Insurance) Portability and Accountability Act (HIPPA) protects the privacy of patients' medical history, that is, if such information is shared with fellow offices that fall under HIPPA law. Similarly, schools must also abide by medical record privacy if they are regulated by the Family Educational Rights and Privacy Act (FERPA). The list

---

[58] Schwartz, "The EU-U.S. Privacy Collision," 1973.

[59] Schwartz, "The EU-U.S. Privacy Collision," 1973.

of very specific data privacy regulations in the US goes on. Much of the privacy security protections in the US are based on circumstantial situations, unlike the EU's particular privacy standards.[60]

Similar to Whitman's observation, Schwartz points out that the First Amendment of the US Constitution protects freedom of speech and, in many ways, can cause a hindrance to freedom of privacy. Americans believe their right to speech outweighs the right to privacy. These beliefs are apparent when it comes to personal data. The US does not place restrictions on data collection or on exporting data out of the country, allowing companies to try new kinds of data processing programs.[61]

There are some cases in which the US depends on the Federal Trade Commission (FTC) to help protect specific data privacy issues. The FTC acts in an advisory role and can only help enforce privacy actions as it does not have jurisdiction to enforce regulations. Still, this does not compare to the EU's privacy standards, which many countries have now replicated into their own governing systems.[62]

In 2012 the EU released an updated proposed privacy legislation called General Data Protection Regulation (GDPR) and the right to be forgotten in hopes of providing better protection over data than previous data privacy laws. As technology develops, new challenges in protecting individual data continue to arise. The GDPR would act as a shield for all data processed, protecting all residents within the EU Member States. This new regulation limits the type of data processed, the purpose for processing, the

---

[60] Schwartz, "The EU-U.S. Privacy Collision," 1971.

[61] Schwartz, "The EU-U.S. Privacy Collision," 1972.

[62] Schwartz, "The EU-U.S. Privacy Collision," 1972.

timeframe in which data can be stored and how the data is stored. Businesses are expected to handle data with the utmost care. The GDPR has created new expectations and, in doing so, raised the global standard for data protection. Any company that violates these standards can be fined up to two percent of the company's worldwide revenues.[63]

As of 2013, the EU has called attention to Google and Facebook for their concerning data privacy practices, and the US' FTC has acknowledged the EU findings. Nevertheless, this observation has not changed or influenced data handling practices in the US or increased the level of privacy protection provided to Americans. The GDPR could, in fact, cause concern between the US and EU relations in the future unless the two governments reach a new data privacy agreement or the US develops federal data privacy laws.[64]

Similar to Schwartz, in his article, "Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with a Private Right of Action," legal scholar Alec Wheatley discusses the many concerns over the lack of US federal data privacy laws. Wheatley opens his article with a harsh reminder for some and a rude awakening for others of a cyberattack where seventy million people were the victims of data theft. Therefore, this article explores how the absence of federal privacy law in the US harms consumers and how unaware most are of the data collecting process.[65]

---

[63] Schwartz, "The EU-U.S. Privacy Collision," 1980.

[64] Schwartz, "The EU-U.S. Privacy Collision," 1988.

[65] Alec Wheatley, "Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with A Private Right of Action," *Golden Gate University Law Review* 45, no. 3 (September 2015): 265-86, https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=2150&context=ggulrev.

Wheatley argues that consumers' desire for information privacy is ignored by the businesses' desire for data collection. The US federal government has yet to implement a national standard that creates a compromise for these opposing expectations. Wheatley continues by acknowledging the dangers of sharing information online. Once consumers give consent, in situations where and when permitted, companies can do as they wish with the data in any regard. Some companies do provide notice-and-consent, also known as "End User License Agreements" or "Terms and Conditions Forms." However, the length of these agreements and the level of comprehension of legal jargon intentionally make it difficult and undesirable for users to read.[66]

These invasive tactics to collect users' data are a far cry from the protection expectations set forth very early on in the US, according to Wheatley. In the 1890s, when the handheld camera was invented, Samuel Warren and Louis Brandeis published the article "The Right to Privacy" to address the new potential of privacy violations. The concepts of the "right to be left alone" and "zones of privacy" were developed regarding family life, but, as Wheatley points out, that conversation changed as businesses are now collecting an unforeseen amount of data via online interactions. A shift has occurred where businesses now have control over privacy expectations.[67]

Wheatley further discusses how the internet has forced a change in privacy dynamics. Pre-internet laws were meant to protect privacy, such as the Privacy Act of 1974, but now hold very little weight against the current technology. However, the US

---

[66] Wheatley, "Do-It-Yourself Privacy," 268.

[67] Wheatley, "Do-It-Yourself Privacy," 270.

has a historical tendency to develop laws after a problem arises instead of implementing precautionary measures. One of the first opportunities the US had to develop standard data privacy regulations was with *In re Doubleclick Inc. Privacy Litigation*. The company used cookies to track its consumers and then target them with advertisements. The court found Doubleclick not guilty of violating consumer privacy because the consumers chose to click on the presented advertisements. By clicking on the advertisement leading to an external website, the user automatically agrees to the company's terms and conditions.[68]

As mentioned by Schwartz, the FTC is an advisory body for data privacy violation enforcement. Wheatley discusses the FTC a bit further by recognizing the Commission's role in enforcing unfair competition regulations. The FTC could oversee data privacy, however, with a limited staff and a limited budget, the FTC is ill-equipped to properly handle privacy violations. Currently there are several problems in how the FTC handles privacy issues, including allowing companies to settle disputes while not reporting any wrongdoing on businesses' behalf. As it stands, the FTC cannot be the solution to consumer data privacy protection. Wheatley thus makes an argument for the need of federal data privacy legislation to combat consumer violations.[69]

In the proposed legislation, he writes that companies would be obligated to provide transparency, accountability, proper consent, a system for internal oversight and the ability to provide remediation and external oversight. These steps will hold businesses accountable and solve consumer data privacy issues in the US. In doing this, the US will

---

[68] Wheatley, "Do-It-Yourself Privacy," 277.

[69] Wheatley, "Do-It-Yourself Privacy," 279-286.

better align with other countries that already enforce data privacy regulations. Federal law would provide some consumer security to the lawless realm of the internet.[70]

The US may not have yet passed federal data privacy legislation, but states within the country have begun taking matters into their own hands. California has enacted the California Consumer Privacy Act (CCPA), which legal scholars Mark A. Rothstein and Stacey A. Tovino describe as "GDPR light" in the article "California Takes the Lead on Data Privacy Law." The CCPA was created and pushed by wealthy Californian Alastair Mactaggart, who spent millions to see this bill enacted. A scaled-back version of the CCPA in 2018 was finally adopted and signed into law by Governor Jerry Brown.[71]

Residents of California have the protection of the CCPA to guard their data against any violations from online businesses collecting data. Such protections include the right to be informed of data collection, the right not to have additional data collected without notice, the right to request data deletion from businesses, and the right to access information about the data collected. However, the CCPA does not protect against all businesses such as nonprofits or healthcare companies but gives consumers the right to protect against most other businesses.[72]

The enactment of the CCPA has led other states to follow suit by developing state-specific data privacy bills for residents, which may help influence the US to adopt federal

---

[70] Wheatley, "Do-It-Yourself Privacy," 285.

[71] Mark A. Rothstein and Stacey A Tovino, "California Takes the Lead on Data Privacy Law," *Hastings Center Report* 49, no. 5 (September 2019): 4-5, https://www.ncbi.nlm.nih.gov/pubmed/31581323.

[72] Rothstein and Tovino, "California Takes the Lead on Data Privacy Law," 4.

data privacy legislation. However, the authors are doubtful this will happen at any time in the foreseeable future because of the complexities involved, such as the current political climate and the costs related to development. The CCPA does provide a benchmark for future data privacy legislation in the US.[73]

The review of these articles has revealed that culturally, both EU and US residents desire privacy, just in different ways. Therefore, privacy laws are needed and desired. The passage below presents a timeline of privacy laws leading to data privacy protections in the EU and the US.

Evolution of Privacy Laws in the EU and US

The EU has had substantial control over enforcing the secure management of consumer data beginning with the United Nations adaptation of the 1948 Universal Declaration of Human Rights, where it is proclaimed that the right to privacy is a fundamental human right.[74] In 1950 all European members adopted this right during the European Convention on Human Rights.[75] Since then, the EU has enacted a series of laws in which protect individuals' data. In 1981 the Convention for the Protection of

---

[73] Rothstein and Tovino, "California Takes the Lead on Data Privacy Law," 5.

[74] The General Assembly, "Universal declaration of human rights." *United Nations,* (1948), https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[75] European Court of Human Right, "Convention for the Protection of Human Rights and the Fundamental Freedoms" (1950). *European Convention on Human Rights*, (1950), https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Individuals with regard to Automatic Processing of Personal Data Treaty No.108 laid down restrictions on the collection, processing and storage of personal data.[76]

The Data Protection Directive (1995) mandates that businesses have a legitimate reason for processing data, provide several protective measures for when data is transferred, maintain responsibility for what happens to the data and protect any identifiable or unidentifiable natural person.[77] Following the Data Protection Directive derived the Telecommunication (Data Protection and Privacy) (Direct Marketing) Regulations 1998,[78] the Privacy and Electronic Communications Directive (2002)[79] and the Data Retention Directive (2006), where both member and nonmember states were expected to comply with each of the EU's Directive to do business with the EU Member States.[80]

---

[76] "The History of the General Data Protection Regulation," European Data Protection Supervisor, https://edps.europa.eu/data-protection/our-work/publications/legislation/directive-9546ec_en. https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en

[77] "The History of the General Data Protection Regulation," European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_enhttps://edps.europa.eu/data-protection/our-work/publications/legislation/directive-9546ec_en.

[78] "The Telecommunications (Data Protection and privacy) (Direct Marketing) Regulations 1998," The National Archives, (December 16, 1998), https://www.legislation.gov.uk/uksi/1998/3170/made.

[79] "The History of the General Data Protection Regulation," European Data Protection Supervisor, https://edps.europa.eu/data-protection/our-work/publications/legislation/directive-9546ec_enhttps://edps.europa.eu/data-protection/our-work/publications/legislation/directive-200258ec_en.

[80] The European Parliament and The Council of The European Union, "Directive 2006/24/EC of the European Parliament and of The Council of 15 March 2006," EUR-Lex, (2006), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0024.

Each of these laws became steppingstones for the proposed General Data Protection Regulation (GDPR) (2012), where the European Commission adopted measures to implement the notification of personal data breaches in 2013.[81] The revised GDPR, enacted in 2018, is the most recent law to enforce data protection for EU residents.[82] It has set groundbreaking standards with the case of Google *Spain SL v. Agencia Española de Protección de Datos*, where it was ruled that Google is responsible for processing personal data. Since Google processes user data similarly to any online business, even though it operates as a free search engine, it should follow EU compliance and grant individuals the right to be forgotten.[83]

As the EU has taken several progressive steps in protecting the safekeeping and proper handling of data, many countries worldwide have begun following in the EU's path of data protection. The EU is currently viewed as the world leader in combating the dangers of technology. Unlike its Western counterpart, the US, the country that introduced the world to the internet and online commerce, has fallen significantly behind in developing data regulations.

---

[81] "The History of the General Data Protection Regulation," European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[82] "The History of the General Data Protection Regulation," European Data Protection Supervisor, https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

[83] Haupt, C. E., Balkin, J. M., "Google Spain SL V. agencia española de protección de datos," *Harvard Law Review*, (December 10, 2014), https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/.

A historical overview of privacy laws in the US shows that American culture supports individual privacy, but governing bodies are slow to legally implement those beliefs. The concept of individual privacy in the US can date back to 1890 when Louis Brandeis and Samuel Warren published the article "The Right to Privacy" in the *Harvard Law Review*. The article calls for the individual's right to protection of personal and property privacy.[84] Additionally, Amendment IV of the US Bill of Rights states that people have the right "to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated."[85] To date, several Supreme Court decisions build upon Amendment IV to protect individuals' privacy.[86] For example, in *Olmstead v. United States* (1928), federal agents wiretapped Roy Olmstead's private phone conversations without judicial approval, later using that evidence to prosecute Olmstead. However, the Supreme Court determined Olmstead's privacy rights had not been violated.[87] *Olmstead v. United States* (1928) was later overturned with *Katz v. United States* (1967), where federal agents wiretapped a telephone booth used by Katz. The court determined an individual has a reasonable expectation of privacy in which this act violates the Fourth Amendment.[88]

---

[84] Daniel J. Solove, "A Brief History of Information Privacy Law," George Washington University Law School (2006): 1-46, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

[85] "The Bill of Rights: What Does It Say?" National Archives and Records Administration, 2020, https://www.archives.gov/founding-docs/bill-of-rights/what-does-it-say.

[86] Solove, "A Brief History of Information Privacy Law," 1-46.

[87] Solove, "A Brief History of Information Privacy Law," 18.

[88] Solove, "A Brief History of Information Privacy Law," 22.

The Privacy Act of 1974 requires government agencies to provide public notice of personal record-keeping and is required to establish a fair code of information practices. The USA Freedom Act (2015) was approved after Edward Snowden, a computer intelligence consultant for the National Security Agency (NSA), publicly revealed the Agency's practices of aggregating bulk metadata from Americans without notification. This Act introduces a Special Advocate to mediate privacy and public matters and provide new privacy protections for the individual. However, bulk collection of metadata and internet data from phone companies are still permissible.[89]

One aspect of cellphone data that cannot be tracked without a warrant is cell site location information, as *Carpenter v. United States* (2018) ruled where a warrant must be mandated before accessing an individual's cell phone coordinates.[90] Other acts enacted but have limitations are the Health Insurance Portability and Accountability Act (HIPPA), where medical records are protected;[91] the Children's Online Privacy Protection Act (COPPA), which protects children and does not allow businesses to collect information of children 12 and under without the consent of a parent;[92] the Gramm-Leach-Bliley Act,

---

[89] Rep. James. F. Sensenbrenner Jr., "H.R.2048 - 114th Congress (2015-2016): USA Freedom Act of 2015." Congress.gov, June 2, 2015. https://www.congress.gov/bill/114th-congress/house-bill/2048.

[90] Nathan Freed Wessler, "The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In," ACLU Massachusetts, July 1, 2019. https://www.aclum.org/en/publications/supreme-courts-most-consequential-ruling-privacy-digital-age-one-year.

[91] Solove, "A Brief History of Information Privacy Law," 37.

[92] Solove, "A Brief History of Information Privacy Law," 38.

protects data privacy and security involving banking;[93] and most recently the California Consumer Privacy Act (CCPA) of 2018, enacted in 2020, which provides residents in the state of California protections to control their personal information online that is often collected by online companies.[94] Businesses and data brokers are now required to provide notices of their privacy policies to consumers. The main four prongs of the CCPA include the right to know, the right to delete, the right to opt-out and the right to non-discrimination.[95]

Literature Summary

With a historical overview of privacy laws in the EU and the US, the cultural and Literature Summary legal implications show that consumers need and desire privacy. However, as technology develops, there is also a clear need and desire for data aggregation by consumers and businesses alike. This view of data aggregation is strengthened by the observations of Varian and McAfee and Brynjolfsson. They believe that data aggregation is a highly-performing, highly-profitable business model that companies will continue to use for the unforeseeable future.

Although data aggregation assists in improving sales and the consumer purchasing experience, there also persists a strong desire for privacy from consumers.

---

[93] "Gramm-Leach-Bliley Act," Federal Trade Commission, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

[94] "California Consumer Privacy Act (CCPA)," State of California - Department of Justice - Office of the Attorney General, (2020), https://www.oag.ca.gov/privacy/ccpa.

[95] "California Consumer Privacy Act (CCPA)."

Zuboff, Nissenbaum and West reveal the near absence of data privacy protections provided by businesses and governing bodies on behalf of consumers. It appears online businesses have imposed a correlation where consumers must give up their privacy to partake online. However, these actions do not need to be mutually exclusive, and laws can help ensure that.

While Zuboff, Nissenbaum and West draw out the issues of data harvesting in the surveillance capitalism model and touch upon potential legal solutions, Whitman, Schwartz and Wheatley discuss the need for government intervention for data privacy law. Whitman shows how the EU and the US are intertwined in many ways yet view individual privacy very differently. Schwartz shows how these governing bodies have handled issues of data privacy involving online tech giants such as Facebook and Google. Although the US agrees with the EU findings of privacy violations, the US has yet to enforce regulations that handle such issues for Americans. However, in California, the CCPA has become the most comprehensive data privacy law in the US to date. Rothstein and Tovino present how the CCPA holds promise for the future development of data privacy protections in the country.

After analyzing the benefits and disadvantages of data aggregation, the lack of data privacy laws for individuals and the clear need for them, it is important to study the current laws that aim to protect consumers' privacy. There is a need to determine if the GDPR or CCPA can address the many privacy concerns listed. Both laws are innovative and novel when dealing with technology and privacy, but which one is better at addressing privacy concerns laid out by Zuboff? Determining which law is better equipped at handling a data privacy scholar's concerns can provide a clear understanding

of what future data privacy laws must aim to include in legislation. A comparison of the GDPR and CCPA can also provide information on the areas in which the law lacks protection.

This thesis aims to answer the question: does the General Data Protection Regulation or the California Consumer Privacy Act better protect individual's data privacy in a surveillance economy? Based on the EU and the US differences of legal and cultural backgrounds presented by the articles in this chapter, it appears that the GDPR is better positioned to address the dangers of surveillance capitalism.

In answering this question, this thesis aims to offer a new prospective of the GDPR and the CCPA for future scholars to build upon. It hopes to provide lawmakers better insight into what areas of data privacy concerns are still missing and need to be addressed. Lastly, and most importantly, answering this question will inform consumers about the necessity of efficient data privacy laws (especially for consumers unaware of data aggregation and their right to data privacy).

Chapter III.

Research Framework and Methods

This chapter discusses the methodological approach used in answering the proposed thesis question: does the General Data Protection Regulation or the California

Consumer Privacy Act better protect individual's data privacy in a surveillance economy? In order to determine if the GDPR or CCPA is better equipped at protecting the data privacy of individuals, each law is compared to Zuboff's concerns as listed in her article "Big other: Surveillance Capitalism and the Prospects of an Information Civilization." Based on the comparison results, the law that addresses a greater number of listed concerns is considered to be better equipped at providing effective data privacy rights and protections for consumers. Before going into further details on how the laws are compared, I first discuss the importance of comparing international laws.

Comparative Law

Why compare laws that govern two separate populations? Legal scholar Edward J. Eberle supports this approach in his article, "The Methodology of Comparative Law." He writes that comparative law is important as a legal science and should be more broadly used. He continues by stating that law can be paired with many disciplines and provide greater context when developing law itself. In addition, as the world continues to be globally linked, it can help improve "…human welfare and our legal order."[96] In a way, the method of comparative law allows us to understand a country's culture and its people better. Eberle breaks down the methodological process of comparative law into four parts:

> (Rule 1) is acquiring the skills of a comparativist in order to evaluate law clearly, objectively, and neutrally…. (Rule 2) is evaluation of the law as it is expressed

[96] Edward J. Eberle, "The Methodology of Comparative Law," Roger Williams University Law Review 16, iss. 1 (2011): 72, 51-72, http://docs.rwu.edu/rwu_LR/vol16/iss1/2.

> concretely, in words, action, or orality.… (Rule 3) of the methodology [is] an evaluation of how the law actually operates within a culture…. (Rule 4) [is] comparative observations that can shed light on both a foreign and our own legal culture.[97]

When gaining the skills of a comparativist, one has to immerse oneself in the historical, political and economic culture to fully understand a country's legal framework. In addition, one must focus on the underlying concepts, beliefs, and reasons to apply Rule 1 successfully. When working on Rule 2, a careful review of each law's context, meaning, and application needs to be performed. Then one must focus on the similarities and differences between the laws and why. Rule 3 allows for a deeper understanding of the law and how it works within society by looking at the legal culture. This rule shows how the laws function beyond legal verbiage and how they are applied in everyday life. The last component is piecing together all the findings for Rule 4. This part comprises bringing together the significance of the data, observations of the legal system, operation rules, efficiency of law and, overall, what was learned by the comparison.[98]

For the purpose of this study, I focus on Rule 2 and analyzing each law to learn more about how the law can address data protection. I then determine the similarities and differences within the cultures to understand the types of verbiage used within the law and remove any language barriers by utilizing words that can be defined with the same meaning. I take careful considerations of the similarities and differences of the language of the laws. The most efficient way of comparing the laws is by understanding their verbiage. Only then can the laws accurately be tested.

---

[97] Eberle, "The Methodology of Comparative Law," 57-58.

[98] Eberle, "The Methodology of Comparative Law," 57.

I analyze the verbiage to determine the areas of data privacy each law addresses. These observations are measured against a Rubric I develop (detailed below). Since I am not as familiar with EU law, I also use Rule 1 to familiarize myself and gain command in understanding the culture and history of the laws shared among the EU Member States. For this study, I only focus on the verbiage of the laws and, therefore, Rule 3 does not apply and is not utilized. After gaining command of the law, Rule 4 is applied by reviewing the result of the comparison of the GDPR and CCPA to the Rubric test. Once all of the above procedures are met, then I test the laws against the Rubric and determine which law better addresses Zuboff's data privacy concerns.

Eberle's methodology of comparative law provides the rationale for proper analysis and comparison of the GDPR and the CCPA. These Rules allow for both laws to be viewed from an equal perspective and therefore compared efficiently. With these Rules, a test can now be performed to determine if the GDPR or CCPA better addresses data privacy protections.

Method of Comparing the GDPR and the CCPA: The Zuboff Rubric

In determining if the GDPR or the CCPA provides better data privacy protection for consumers, I compare the laws to a list of concerns presented by Zuboff in her article "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization". I separate the list into two tables, (Table 1) implicit solutions for current asymmetries of knowledge and power and (Table 2) implicit solutions to legitimatize detection and sanctions between businesses and consumers. I choose to base the categories of the two

tables on Zuboff's scholarship because of her extensive and innovative research into surveillance capitalism and the data harvesting methods performed by businesses.

Zuboff's work stems back to the 1980s, aligning with the introduction of the internet in homes and has followed the progress of businesses and the internet ever since. She has produced several articles and books on technology and privacy ranging from *In the Age of the Smart Machine: The Future of Work and Power*, predicting the significance of computers in the workplace to her most recent book, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, which discusses the technology-based challenges humanity now faces. Zuboff is the Charles Edward Wilson Professor Emerita at Harvard Business School and a former Faculty Associate at the Berkman Klein Center for Internet and Society at Harvard Law School. Her decades of research and experience prove Zuboff's knowledge on data privacy to be well qualified for developing a rubric test based on her scholarship of data privacy concerns.[99]

In the article "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization" there are several asymmetries and lack of solutions between businesses and consumers mentioned. I list discussion points from the article under one of the two groups. The first group is categorized under asymmetries of knowledge that I add to Table 1, titled "Zuboff Rubric: Implicit Solution for Current Asymmetries of Knowledge & Power in Business/Consumer Transactions." For the second category Zuboff does not explicitly list direct solutions but rather a lack of detection and sanctions

[99] "About," Shoshana Zuboff.com, https://shoshanazuboff.com/book/shoshana/.

to describe when businesses violate data privacy protections. For the lack of detection and sanctions, I create a list of implied ways they could be enforced by authority for Table 2, titled "Zuboff rubric: Implicit Solutions to Legitimatize Detection & Sanctions in Business/Consumer Transactions."

I then take the two above lists to develop the Zuboff Rubric.[100] In order to determine if the GDPR or CCPA meets the requirements of the Zuboff Rubric,[101] I look for articles within each law to match keywords or phrases within each term solution listed in Table 1 and Table 2. The closer the article mirrors the meaning of the term description in its entirety, the better equipped it is at addressing the listed concern. Each listed concern has four adjacent categories to determine the level of solution fulfillment. The list of solution fulfillment categories are defined as follows:

- **Clearly Absent of Solution** - there is no mention of or reference to term solution within the law, therefore, not addressed;
- **Indirect Reference to Solution** - the law mentions or references the concern but is negligent in providing a solution; the term's solution is implied but negligible;
- **Direct Reference to Solution** - the law mentions or references the concern, and a solution is implied but not to the fullest extent; the term's solution is implied or suggested but is not explicitly addressed;

---

[100] Zuboff, "Big Other," 75-89.

[101] Zuboff, "Big Other," 75-89.

- **Explicitly Addresses Solution** - the law explicitly mentions or references the concern, shows direct evidence of addressing a solution.

After a thorough overview of the law, a checkmark is then placed in one of the four adjacent columns to track the level of fulfillment for each term. A sixth column lists the accompanying article within the law used to determine the level of solution fulfillment. If no article within the law matches the list of concerns, then the concern is "Clearly Absent of Solution." In this case where articles are "Clearly Absent of Solution," the article column is left blank due to the lack of an existing article. The comparison section in Chapter IV provides a results table guide with the number of times an article met each solution level addressed.

I measure the GDPR and the CCPA individually against Zuboff Rubric in Table 1 and Table 2 through a thorough analysis of legal texts. A short description and reasoning for applying the article to the Solution are provided after each table.*

The specific laws that I analyze are:

- Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data on the free movement of such data and repealing

Directive 95/46/EC (General Data Protection Regulation). The law consists of 11 chapters, 99 articles and 173 Recitals spanning over 88 pages.[102]

- TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100-1798.199]. The law consists of 24 articles spanning over 17 pages.[103]

Although having the same meaning, six instrumental terms within the GDPR and the CCPA differ. In this case, I chose to utilize three terms to be used consistently throughout the analysis for simplicity. The GDPR uses the term "subject,"[104] and the CCPA uses the term "consumer."[105] For simplicity, I use the term consumer. Consumers are individuals who utilizes the internet for various purposes and have their data collected.

---

*I should note that I do not possess a Juris Doctor degree or a background in legal studies at the time of writing this thesis. However, if these laws are meant to share a level of transparency with consumers and protect all consumers regardless of reading level, then my understanding of the law should hold appropriate grounds for analysis.

[102] "General Data Protection Regulation (GDPR)," GDPR.eu, https://gdpr.eu/tag/gdpr/.

[103] "California Consumer Privacy Act (CCPA), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4."

[104] "General Data Protection Regulation (GDPR)."

[105] "California Consumer Privacy Act (CCPA)."

The GDPR uses the term "data controller" and "data processor,"[106] and the CCPA uses the term "business."[107] I use the term business. To clarify, a business refers to a natural or legal person, regardless of the size of business, for-profit or nonprofit, public or private are all held accountable to uphold proper data regulations.[108]

The GDPR uses the term "processing data,"[109] and the CCPA uses the term "collect."[110] I use "processing data." To process data means to gather and utilize information from a consumer. Data is any identifiable information of a consumer. Additionally, the articles within the laws are too long to place within the rubric. Instead, I use the article number and section within the rubric. The full list of articles can be found in Appendix I GDPR and Appendix II CCPA at the end of the thesis for more clarity.

After a complete analysis and comparison of the GDPR and the CCPA articles to the list of concerns of the Zuboff Rubrics,[111] the law with more checks under Explicitly Address Solution is considered the law to better address Zuboff's concerns. The law that better addresses Zuboff's concerns is also considered the law better equipped at providing data protection for consumers.

---

[106] "General Data Protection Regulation (GDPR)."

[107] "California Consumer Privacy Act (CCPA)."

[108] "General Data Protection Regulation (GDPR)."

[109] "General Data Protection Regulation (GDPR)."

[110] "California Consumer Privacy Act (CCPA)."

[111] Zuboff, "Big Other," 75-89.

TABLE 1
ZUBOFF RUBRIC: IMPLICIT SOLUTIONS FOR CURRENT ASYMMETRIES OF KNOWLEDGE & POWER IN BUSINESS / CONSUMER TRANSACTIONS

Implicit Solutions For Current Asymmetries of Knowledge & Power in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution
Businesses Should Provide Consumers with the Ability to Opt-Out of Data Collection	☐	☐	☐	☐
Businesses Should Provide Consumers with Data Collection Transparency (data: type, purpose, experiments, timeframe of storage, location of storage)	☐	☐	☐	☐
Businesses Should Provide Consumers with a Contractual Consent Agreement Before or at the Time of Data Collection	☐	☐	☐	☐
Businesses Should Inform Consumers of any Algorithm Predictor Used to Determine Consumer Preferences	☐	☐	☐	☐
Businesses Should Provide Consumers an Alternative Payment Methods for Online Services (In Lieu of Data Collection as Payment)	☐	☐	☐	☐
Businesses Should Offer Consumers the Option of Data Deletion from Company Database	☐	☐	☐	☐
Businesses Should Provide Consumer Control Over How Their Personal Data is Utilized and With Whom	☐	☐	☐	☐

Source: Shoshana Zuboff. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Explicitly Addresses Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

TABLE 2
ZUBOFF RUBRIC: IMPLICIT SOLUTIONS TO LEGITIMATIZE DETECTION & SANCTIONS IN BUSINESS / CONSUMER TRANSACTIONS

Implicit Solutions to Legitimize Detection & Sanctions in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution
Government Should Offer Mechanism for Consumers to Report Data Privacy Violations from Businesses	☐	☐	☐	☐
Businesses Should Provide Consumer Contract for Data Collection, Usage, and Sale	☐	☐	☐	☐
Businesses Should Have Company Practices and Guidelines Available to Consumers (data: collection, algorithms, sales, experimentations, storage)	☐	☐	☐	☐
Businesses Should Provide Consumers with Easy to Understand Contracts	☐	☐	☐	☐
Government Should Enforce Hefty Fines or Suspension of Service and Order Deletion of Unauthorized Consumer Data when Businesses Violate Consumers' Data Privacy Rules	☐	☐	☐	☐

Source: Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Mentions Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

Chapter IV.

Comparison of the General Data Protection Regulation and the California Consumer Privacy Act

But if it's only in your feed, between you and Facebook, and their microtargeting of who you are, that's not democracy anymore…. That's just privatised de facto manipulation of who you're going to vote for.

- Margrethe Vestager, European Competition Commissioner[112]

This chapter looks at the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) to determine which law better addresses consumer data privacy protections for consumers who engage with businesses online. Each law is reviewed against the list of concerns presented by Zuboff and is measured by the Zuboff Rubric[113] as detailed in Chapter III. The law that addresses a higher number of "Explicitly Addresses Solution" determines which law resolves more of Zuboff's concerns and, therefore, is better equipped at providing consumer data privacy protections.

Comparing the GDPR and CCPA to the Zuboff Rubric reveals that the GDPR fulfills more (table 5) "Explicitly Addresses Solution" within the Zuboff Rubric than the CCPA does (table 3). Of the twelve listed items between the two Zuboff Rubrics, the GDPR articles satisfy "Explicitly Addresses Solutions" four times, "Direct Reference to

---

[112] Victoria Waldersee, "EU's Vestager Backs Twitter for Banning Political Ads, Berates Facebook," Reuters, November 7, 2019, https://www.reuters.com/article/us-eu-antitrust-twitter-facebook-idUSKBN1XH2I2.

[113] Zuboff, "Big Other," 75-89.

Solution" six times and "Clearly Absent of Solution" two times and does not provide an "Indirect Reference to Solution." The CCPA satisfies "Explicitly Mentions Solutions" three times, "Direct Reference to Solution" two times, "Indirect Reference to Solution" five times and "Clearly Absent of Solution" two times. Based on the measurement of the Zuboff Rubric, the GDPR is better equipped at protecting consumer data privacy rights.

TABLE 3

ZUBOFF RUBRIC: IMPLICIT SOLUTIONS FOR CURRENT ASYMMETRIES OF KNOWLEDGE & POWER IN BUSINESS / CONSUMER TRANSACTIONS BASED ON THE GENERAL DATA PROTECTION REGULATION (GDPR)

Implicit Solutions For Current Asymmetries of Knowledge & Power in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution	General Data Protection Regulation Article (Solution)
Businesses Should Provide Consumers with the Ability to Opt-Out of Data Collection	☐	☐	☐	☑	**Art. 21 GDPR, Art. 22 GDPR**
Businesses Should Provide Consumers with Data Collection Transparency (data: type, purpose, experiments, timeframe of storage, location of storage)	☐	☐	☑	☐	**Art. 12 GDPR, Art. 13 GDPR, Art.15 GDPR**
Businesses Should Provide Consumers with a Contractual Consent Agreement Before or at the Time of Data Collection	☐	☐	☑	☐	**Art. 6 GDPR, Art. 7 GDPR, Art. 18 GDPR, Art. 21 GDPR**
Businesses Should Inform Consumers of any Algorithm Predictor Used to Determine Consumer Preferences	☐	☐	☐	☑	**Art. 15 GDPR**
Businesses Should Provide Consumers an Alternative Payment Methods for Online Services (In Lieu of Data Collection as Payment)	☑	☐	☐	☐	
Businesses Should Offer Consumers the Option of Data Deletion from Company Database	☐	☐	☐	☑	**Art. 17 GDPR**
Businesses Should Provide Consumer Control Over How Their Personal Data is Utilized and With Whom	☑	☐	☐	☐	

See Appendix for Articles of the GDPR

Source: "GDPR Archives." GDPR.eu. Accessed April 27, 2016. https://gdpr.eu/tag/gdpr/.

Source: Shoshana Zuboff. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89. https://doi.org/10.1057/jit.2015.5.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Mentions Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

Results of the Zuboff Rubric: Implicit Solutions for Current Asymmetries of Knowledge and Power in Business/Consumer Transactions Based on the General Data Protection Regulation (GDPR)

Businesses Should Provide Consumers the Ability to Opt-Out of Data Collection — (Explicitly Addresses Solution)

The law "Explicitly Addresses Solution" because consumers can object (or "opt-out") to having their data processed. The term "opt-out" is not mentioned, but the term "object" is used to imply refusal of data processing. A consumer may choose to opt-out of data collection at any time. There are certain circumstances in which a business does not need to comply if the business can prove a compelling reason to continue processing the data.[114]

Under "Article 21 GDPR Right to object," consumers have the right to put a stop to all processing of data that pertains to themselves unless a business has "compelling legitimate grounds" to process such data. Consumers have the right at any time to deny processing, except in the case of serving a greater public interest. An objection to processing includes the purpose of marketing.[115]

Although not directly addressing the concern, consumers have the right not to be profiled based solely on an automated process. Businesses profile consumers based on

---

[114] "General Data Protection Regulation (GDPR)."

[115] "General Data Protection Regulation (GDPR)."

their online habits, which assists businesses in targeting advertisements to consumers most likely to purchase a specific item. "Article 22 GDPR Automated individual decision-making, including profiling" provides consumers the right not to be profiled. This ability allows consumers not to be subjected to decisions offered by businesses based on data algorithms.[116]

Businesses Should Provide Consumers with Data Collection Transparency (data: type, purpose, experiments, timeframe of storage, location of storage) — (Direct Reference to Solution)

The law comes close to fulfilling this term by requiring specific information to be provided to consumers at the time of data processing. However, it does not require all the data information as listed in the term. The law does not include information on experimentations performed, but consumers have the right to be informed of automated decision-making (a form of experimentation).[117]

The requirements include the categories of personal data, the purpose of processing the data and the criteria determining the storage timeframe. The law does not include information on experimentations performed with the processed data but mentions that consumers have the right to be informed of automated decision-making. This is where experiments are necessary to provide such a process.[118]

---

[116] "General Data Protection Regulation (GDPR)."

[117] "General Data Protection Regulation (GDPR)."

[118] "General Data Protection Regulation (GDPR)."

"Article 13 GDPR Information to be provided where personal data are collected from the data subject" requires businesses to provide information pertaining to consumers' data at the time of processing. Businesses must inform consumers of the following: the purpose of data collection and its legal basis for processing, the length the data will be stored, contact details of the data processor and third-party vendors, safeguards put into place when businesses sell data to third-party countries and any existence of automated decision-making.[119]

"Article 15 GDPR Right of access by the data subject" allows consumers to obtain a copy of the information mentioned in Article 13 from businesses.[120]

"Article 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject" forces businesses to take appropriate actions to ensure consumers are provided with information pertaining to the processing of data. When providing information to a customer, the information must be transparent and intelligible using a simple language form to assure consumers' complete comprehension. A business must respond to data inquiry requests within a month of receiving the request or provide the consumer with a reason for not providing such information. In failing to provide a response, businesses face the possibility of consumers filing a complaint with a supervisory authority and facing judicial action. The business must provide a free copy of the data report unless a consumer requests information excessively. If the business cannot

---

[119] "General Data Protection Regulation (GDPR)."

[120] "General Data Protection Regulation (GDPR)."

accurately identify consumers requesting a data report, then the business is not obligated to provide such information.[121]

Businesses Should Provide Consumers with a Contractual Consent Agreement Before or at the Time of Data Collection — (Direct Reference to Solution)

Businesses providing consumers with a contract for data processing is not explicitly mentioned within the law. However, this law does provide a "Direct Reference to Solution" as businesses do need to inform consumers of processing and in some cases, a consumer needs to provide consent for processing. For cases where consent is not necessary, businesses need evidence that the data processed assists with the transaction performance for consumers.[122]

"Article 6 GDPR Lawfulness of processing" only allows businesses to process data if one of the following conditions are met: consumers provide consent, it is necessary for the performance of the business transaction, follows legal compliance, protects the vital interest of consumers, benefits the public interest or is absolutely necessary.[123]

"Article 7 Conditions for consent" requires a business to be able to provide evidence of consent to processing data if consent is required for processing. The Article also allows for consumers to withdraw consent whenever they wish.[124]

---

[121] "General Data Protection Regulation (GDPR)."

[122] "General Data Protection Regulation (GDPR)."

[123] "General Data Protection Regulation (GDPR)."

[124] "General Data Protection Regulation (GDPR)."

"Article 18 GDPR Right to restriction of processing" allows consumers to restrict the collection and processing of data under four categories: if the data is inaccurate, the processing is unlawful, consumers decide to restrict instead of having the data erased, the company no longer needs the data or if consumers object to the processing.[125]

"Article 21 GDPR Right to object" allows consumers to object to having data processed for marketing. Consumers are also allowed to refuse collection at any time, even after agreeing to the collection, making consumers' consent void.[126]

Businesses Should Inform Consumers of any Algorithm Predictor Used to Determine Consumer Preferences — (Explicitly Addresses Solution)

The law states that businesses need to inform consumers of automatic decision-making and profiling, which are used as predictors to evaluate consumers' habits for targeted marketing. Although not directly mentioned, algorithms are what make profiling possible.[127]

"Article 15 GDPR Right of access by the data subject" businesses must make clear if "automated decision-making, including profiling," is present. Businesses also must provide a significant reason for this practice.[128]

---

[125] "General Data Protection Regulation (GDPR)."

[126] "General Data Protection Regulation (GDPR)."

[127] "General Data Protection Regulation (GDPR)."

[128] "General Data Protection Regulation (GDPR)."

Businesses Should Provide Consumers an Alternative Payment Methods for Online Services (In Lieu of Data Collection as Payment) — (Clearly Absent of Solution)

Alternative payment would allow consumers to pay for services instead of having their data collected. This concern has not been addressed within the legal document and therefore does apply in this situation.[129]

Businesses Should Offer Consumers the Option of Data Deletion from Company Database — (Explicitly Addresses Solution)

The law "Explicitly Addresses Solution" of data deletion by providing consumers "the right to be forgotten." Consumers can request to have personal data deleted from businesses' storage databases. Consumers can request this at any time.[130]

"Article 17 GDPR Right to erasure ('right to be forgotten')" allows consumers the right to contact businesses and have the business delete all data pertaining to consumers making the request. However, companies may continue processing data under certain circumstances such as freedom of expression, compliance with the Member State, public interest or archiving purposes or legal claims.[131]

Businesses Should Provide Consumer Control Over How Their Personal Data is Utilized and With Whom — (Clearly Absent of Solution)

---

[129] "General Data Protection Regulation (GDPR)."

[130] "General Data Protection Regulation (GDPR)."

[131] "General Data Protection Regulation (GDPR)."

The law has articles that permit consumers to withdraw consent of having their data collected. However, there are no articles that provide consumers with the ability to choose how their data is used and with whom it is shared, making it "Clearly Absent of Solution."[132]

[132] "General Data Protection Regulation (GDPR)."

TABLE 4
ZUBOFF RUBRIC: IMPLICIT SOLUTIONS TO LEGITIMIZE DETECTION & SANCTIONS IN BUSINESS / CONSUMER TRANSACTIONS BASED ON THE GENERAL DATA PROTECTION REGULATION (GDPR)

Implicit Solutions to Legitimize Detection & Sanctions in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution	General Data Protection Regulation Article (Solution)
Government Should Offer Mechanism for Consumers to Report Data Privacy Violations from Businesses	☐	☐	☐	☑	**Art. 77 GDPR**
Businesses Should Provide Consumers with a Contract for Data Collection, Usage and Sale	☐	☐	☑	☐	**Art. 6 GDPR, Art. 21 GDPR**
Businesses Should Have Company Practices and Guidelines Available to Consumers (data: collection, algorithms, sales, experimentations, location and timeframe of storage)	☐	☐	☑	☐	**Art. 12 GDPR, Art. 13 GDPR**
Businesses Should Provide Consumers with Easy to Understand Contracts	☐	☐	☑	☐	**Art. 12 GDPR**
Government Should Enforce Hefty Fines or Suspension of Service and Order Deletion of Unauthorized Consumer Data when Businesses Violate Consumers' Data Privacy Rules	☐	☐	☐	☑	**Art. 79 GDPR, Art. 82 GDPR, Art. 83 GDPR, Art. 84 GDPR**

See Reference for Articles of the GDPR

Source: "GDPR Archives." GDPR.eu. Accessed April 27, 2016. https://gdpr.eu/tag/gdpr/.

Source: Shoshana Zuboff. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89, https://doi.org/10.1057/jit.2015.5.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Mentions Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

Results of the Zuboff Rubric: Implicit Solutions to Legitimatize Detection and Sanctions in Business/Consumer Transactions Based on General Data Protection Regulation (GDPR)

Government Should Offer Mechanism for Consumers to Report Data Privacy Violations from Businesses — (Explicitly Addresses Solution)

The law "Explicitly Addresses Solution" by allowing consumers to file a complaint with the proper authority if they find that a business has violated their data privacy.

"Article 77 GDPR Right to lodge a complaint with a supervisory authority" allows for consumers to file a complaint with the supervisory authority within the Member State of their residence or place of work. The Member States' supervisory authority then declares the outcome of the complaint, which may include judicial remedy.[133]

Businesses Should Provide Consumers with a Contract for Data Collection, Usage, and Sale — (Direct Reference to Solution)

The law does not enforce businesses to provide consumers with a contract. However, the law does provide a "Direct Reference to Solution" by not permitting

[133] "General Data Protection Regulation (GDPR)."

businesses to process data without consumer consent or processing purposes. Consumers are informed of processing upon collection and can decide whether or not to consent.[134]

"Article 6 GDPR Lawfulness of processing" allows businesses to process data only under specific circumstances. This includes consumer consent, the necessity to perform a task for consumers, legal purposes, protection of consumers, or if there is a public interest.[135]

"Article 21 Right to object" allows consumers to refuse the collection of data performed by businesses. The article does not explicitly mention that consumers have the right to reject the sale of data to third parties. However, it does state that consumers have the right to refuse data collection for marketing purposes, indicating the inclusion of sales to third-party vendors.[136]

Businesses Should Have Company Practices and Guidelines Available to Consumers (data: collection, algorithms, sales, experimentations, location and timeframe of storage) — (Direct Reference to Solution)

Specific company practices and guidelines are not required to be shared with consumers by law. However, it stipulates those businesses are required to share information surrounding data processing with consumers, providing a "Direct Reference to Solution." The required information does not include algorithms, experimentations,

---

[134] "General Data Protection Regulation (GDPR)."

[135] "General Data Protection Regulation (GDPR)."

[136] "General Data Protection Regulation (GDPR)."

and data storage location, leaving consumers unaware of certain aspects of the data process. [137]

"Article 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject" requires businesses to inform consumers of details pertaining to data processing. The information provided must be done so in a transparent, intelligible way using clear and plain language. The only scenario in which businesses do not have to provide such information is when consumers request a report on the information but cannot verify their identity.[138]

"Article 13 GDPR Information to be provided where personal data are collected from the data subject" mandates that businesses inform consumers on the data process, which include the purpose of data collection, the categories of the recipients of data, the storage period of data and contact of the data protection within the business. This article ensures consumers are provided with a level of data processing transparency. However, it does not offer details on all aspects of processing, such as storage location, types of algorithm methods and information on experimentations of the data.[139]

Businesses Should Provide Consumers with Easy to Understand Contracts — (Direct Reference to Solution)

The law does not require businesses to provide consumers with an official contract for data processing. However, for businesses to process data, consumers must

---

[137] "General Data Protection Regulation (GDPR)."

[138] "General Data Protection Regulation (GDPR)."

[139] "General Data Protection Regulation (GDPR)."

consent to the processing or there must be a legally compelling reason to process. Before or at the time of processing, businesses must inform consumers of such action with straightforward and easy-to-read language.[140]

"Article 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject" ensure that businesses provide any information or communication in relation to the data processing to consumers. All details must be provided in plain language that is transparent and intelligible.[141]

"Article 13 GDPR Information to be provided where personal data are collected from the subject" provides consumers with data processing information. This information includes contact details of the controller and protection officer, the purpose of data collection, legitimate interest for processing, information on recipients of the data and if the data will be transferred to a third party for processing. Additional information includes timeframe of storage, right to withdraw consent, the right to have data erased from the business' database and the ability to file a complaint.[142]

Government Should Enforcement Hefty Fines or Suspension of Service and Order Deletion of Unauthorized Consumer Data when Businesses Violate Consumers' Data Privacy Rules — (Explicitly Addresses Solution)

The law "Explicitly Addresses Solution", as it permits consumers who believe their data privacy rights have been violated by a business to request a supervisory

---

[140] "General Data Protection Regulation (GDPR)."

[141] "General Data Protection Regulation (GDPR)."

[142] "General Data Protection Regulation (GDPR)."

authority for a judicial remedy to rectify the violation. The courts can rectify the violation as seen fit, including enforcement of a fine that can equal anywhere from 2 to 4 percent of the business' annual turnover depending on if the business was aware of the violation.[143]

"Article 79 GDPR Right to an effective judicial remedy against a controller or processor" allows consumers the right to an effective judicial remedy if their rights have been infringed upon.[144]

"Article 82 Right to compensation and liability" allows consumers the right to compensation if the court finds that the business has violated data privacy rights. If found guilty, the business can face a fine of either 10 million EUR or 2 percent of the total worldwide annual turnover, whichever is higher. If the business is found guilty to have knowingly violated consumers' privacy rights, the court can fine the business 20 million EUR or 4 percent of the annual turnover, whichever is higher.[145]

"Article 83 GDPR General conditions for imposing administrative fines" provides perimeters for businesses that have violated consumers' data privacy rights. The level of knowledge and responsibility of the business is taken into account by the supervisory authority. If found guilty, the business can face a fine of either 10 million EUR or 2 percent of the total worldwide annual turnover, whichever is higher. If the business is

---

[143] "General Data Protection Regulation (GDPR)."

[144] "General Data Protection Regulation (GDPR)."

[145] "General Data Protection Regulation (GDPR)."

found to have knowingly violated consumers' privacy rights, the court can fine the business 20 million EUR or 4 percent of the annual turnover, whichever is higher.[146]

"Article 84 GDPR Penalties" Member States shall create the penalties applicable for the infringement of the Regulations. Member States also have the authority to take necessary measures to ensure consumers' protection, which may include fining the business.[147]

---

[146] "General Data Protection Regulation (GDPR)."

[147] "General Data Protection Regulation (GDPR)."

TABLE 5

ZUBOFF RUBRIC: IMPLICIT SOLUTION FOR CURRENT ASYMMETRIES OF KNOWLEDGE & POWER IN BUSINESS / CONSUMER TRANSACTIONS BASED ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Implicit Solutions For Current Asymmetries of Knowledge & Power in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution	California Consumer Privacy Act Article (Remedy)
Businesses Should Provide Consumers with the Ability to Opt-Out of Data Collection	☐	☑	☐	☐	**1798.120.** (a), (b), (c) **1798.135.** (entirety)
Businesses Should Provide Consumers with Data Collection Transparency (data: type, purpose, experiments, timeframe, storage)	☐	☐	☑	☐	**1798.100.** (a), (b), (c), (d) **1798.110.** (a 1-5), (b), (c 1-5) **1798.115.** (a 1-3) **1798.130.** (entirety)
Businesses Should Provide Consumers with a Contractual Consent Agreement Before or at the Time of Data Collection	☐	☑	☐	☐	**1798.100.** (b) **1798.120.** (a), (b)
Businesses Should Inform Consumers of any Algorithm Predictor Used to Determine Consumer Preferences	☑	☐	☐	☐	
Businesses Should Provide Consumers an Alternative Payment Methods for Online Services (In Lieu of Data Collection as Payment)	☑	☐	☐	☐	
Businesses Should Offer Consumers the Option of Data Deletion from Company Database	☐	☐	☐	☑	**1798.105.** (a), (b), (c), (d 1-9)
Businesses Should Provide Consumer Control Over How Their Personal Data is Utilized and With Whom	☐	☐	☑	☐	**1798.105.** (a), (b), (c), (d 1-9), **1798.120.** (a), (b)

See Reference for Articles of the CCPA

Source: "Code Section Group." Codes Display Text. September 23, 2018. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Source: Shoshana Zuboff. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89, https://doi.org/10.1057/jit.2015.5.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Mentions Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

Results of the Zuboff Rubric: Implicit Solutions for Current Asymmetries of Knowledge and Power in Business/Consumer Transactions in Based on the California Consumer Privacy Act (CCPA)

Businesses Should Provide Consumers the Ability to Opt-Out Option of Data Collection — (Indirect Reference to Solution)

The law provides an Indirect Reference to Solution by enforcing businesses to allow consumers to opt-out of having their data sold or shared with third parties. However, consumers are not able to refuse online businesses from processing data.[148]

"Article 1798.120" states that consumers have the right at any time to inform businesses of the refusal of selling or sharing their data with third parties, even after initially opting-in to allow businesses to sell or share data processed.[149]

"Article 1798.135" requires businesses to provide an opt-out choice link visible to consumers on the website homepage. This choice must be provided through a clear and conspicuous link titled "Do Not Sell My Personal Information".[150]

Businesses Should Provide Consumers with Data Collection Transparency (data: type, purpose, experiments, timeframe of storage, location of storage) — (Direct Reference to Solution)

---

[148] "California Consumer Privacy Act (CCPA)."

[149] "California Consumer Privacy Act (CCPA)."

[150] "California Consumer Privacy Act (CCPA)."

The law provides a "Direct Reference to Solution" because businesses are not required to share all the listed items with consumers. However, the information required must be provided by the business to consumers at or before the time of processing. This information includes categories of data to be processed, if the data are sold or shared, the timeframe the data will be stored and the purpose of collection. Consumers may also send in a request to businesses for disclosure details on the data processed. The law does not mention businesses needing to disclose the location of storage and the types of experiments performed with the data.[151]

"Article 1798.100" states that businesses shall provide consumers before or at the time of data processing information on the processing, such as the categories of data collected, timeframe of storage, if the processing includes sensitive information and if the data is shared or sold to third parties. This article gives consumers the right to submit a request to businesses for a free report regarding the information on the categories and personal information collected.[152]

"Article 1798.110" allows consumers to request that businesses disclose information on the categories of data processed, the categories of sources from where the data was collected from, the purpose of collection and the categories of third parties that will receive the data.[153]

"Article 1798.115" allows consumers to request information on the data that is sold and replicates the types of information as detailed in "Article 1798.110". A consumer

[151] "California Consumer Privacy Act (CCPA)."

[152] "California Consumer Privacy Act (CCPA)."

[153] "California Consumer Privacy Act (CCPA)."

also has the right to request businesses disclose if the data will be shared or sold and the categories of third parties receiving the data.[154]

"Article 1798.130" enforces that businesses must provide consumers with at least two or more visible methods to file information requests. Businesses must respond to the request within 45 days of receiving it and comply as long as the requestor's identity is verifiable.[155]

Businesses Should Provide Consumers with a Contractual Consent Agreement Before or at the Time of Data Collection — (Indirect Reference to Solution)

The law does not require businesses to provide consumers with a contract for collecting data. Businesses, however, are expected to inform consumers if data processing occurs and the details involved in the process before or at the time of processing, providing an "Indirect Reference to Solution" to consumers. The law also requires businesses to provide consumers with the choice of having their data sold to third parties.[156]

"Article 1798.100" states that businesses must inform consumers at or before the point of processing data that the processing will occur and provide details of the processing. The details include the categories of processed data, the timeframe the data

---

[154] "California Consumer Privacy Act (CCPA)."

[155] "California Consumer Privacy Act (CCPA)."

[156] "California Consumer Privacy Act (CCPA)."

will be stored, the purpose for processing the data, if the data will be shared or sold and the categories of third parties to receive the data.[157]

"Article 1798.120" requires businesses to provide consumers with a visible link on the front page of their website written as "Do Not Sell or Share My Personal Information," allowing consumers to opt-out of the sharing or selling of their data to third parties.[158]

Businesses Should Inform Consumers of an Algorithm Predictor Used to Determine Consumer Preferences — (Clearly Absent of Solution)

The law does not mention or reference the need for businesses to inform consumers about algorithm predictors. This concern is therefore not addressed.[159]

Businesses Should Provide Consumers an Alternative Payment Methods for Online Services (In Lieu of Data Collection as Payment) — (Clearly Absent of Solution)

Alternative payment is not mentioned or referenced in this body of law and, therefore, does not address this asymmetry.[160]

---

[157] "California Consumer Privacy Act (CCPA)."

[158] "California Consumer Privacy Act (CCPA)."

[159] "California Consumer Privacy Act (CCPA)."

[160] "California Consumer Privacy Act (CCPA)."

Businesses Should Offer Consumers the Option of Data Deletion from Company Database — (Explicitly Mentions Solution)

The law "Explicitly Mentions Solution" by providing consumers with the right to request that a business delete any personal data processed on the business' database, including subdivisions of the business. Certain circumstances may prevent the request for data deletion.[161]

"Article 1798.105" allows consumers the right to request businesses to delete personal data processed by the business. This deletion request includes the records maintained by any subdivision of the business. There are specific stipulations in which businesses may not be required to comply, such as a security incident, a need for a debugging repair, completing the transaction, exercising free speech, serving the public's interest or fulfilling a legal obligation.[162]

Businesses Should Provide Consumer Control Over How Their Personal Data is Utilized and With Whom — (Indirect Reference to Solution)

The law does not explicitly provide consumers with control over how their data is utilized and with whom. However, it does allow consumers to decide if they want their data to be shared or sold to third parties, which provides an "Indirect Reference to Solution" for consumers. By providing consumers with the choice of data sale to third parties, consumers are given some authority over their information. Once permission is

---

[161] "California Consumer Privacy Act (CCPA)."

[162] "California Consumer Privacy Act (CCPA)."

granted for businesses to share and sell data, consumers have no control over what data is shared or sold and with whom it is shared or sold. Consumers do have the right to opt-out of the sharing and selling of their data to third parties and to request for their data to be completely deleted.[163]

"Article 1798.120" forces businesses to provide consumers with an opt-out choice over the sale of their data to third parties.[164]

"Article 1798.105" provides consumers the right to request the deletion of their data from all business databases, including subdivisions of the business.[165]

---

[163] "California Consumer Privacy Act (CCPA)."

[164] "California Consumer Privacy Act (CCPA)."

[165] "California Consumer Privacy Act (CCPA)."

TABLE 6
ZUBOFF RUBRIC: IMPLICIT SOLUTIONS TO LEGITIMATIZE DETECTION & SANCTIONS IN BUSINESS / CONSUMER TRANSACTIONS
BASED ON THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Implicit Solutions to Legitimize Detection & Sanctions in Business / Consumer Transactions	Clearly Absent of Solution	Indirect Reference to Solution	Direct Reference to Solution	Explicitly Addresses Solution	California Consumer Privacy Act Article (Solution)
Government Should Offer Mechanism for Consumers to Report Data Privacy Violations from Businesses	☐	☐	☐	☑	**1798.150.** (a) (1 A, B, C, a), (2) (b)
Businesses Should Provide Consumers with a Contract for Data Collection, Usage and Sale	☐	☑	☐	☐	**1798.100.** (b) **1798.120.** (a), (b) **1798.135.** (a), (1)
Businesses Should Have Company Practices and Guidelines Available to Consumers (data: collection, algorithms, sales, experimentations, location and timeframe of storage)	☐	☑	☐	☐	**1798.100.** (a), (b) **1798.110.** (a), (1-5) (c) (1-5) **1798.115.** (a), (1-3) (b)
Businesses Should Provide Consumers with Easy to Understand Contracts	☐	☑	☐	☐	**1798.135.** (a), (1)
Government Should Enforce Hefty Fines or Suspension of Service and Order Deletion of Unauthorized Consumer Data when Businesses Violate Consumers' Data Privacy Rules	☐	☐	☑	☐	**1798.150.** (a), (1), (A), (B), (C), (2), (b) **1798.155.** (a), (b), (c)

See Reference for Articles of the CCPA

Source: "Code Section Group." Codes Display Text. September 23, 2018. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

Source: Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," Journal of Information Technology 30, no. 1 (2015): pp. 75-89. https://doi.org/10.1057/jit.2015.5.

Terms

Clearly Absent of Solution - no mention of or reference to term solution within the law, not addressed.

Indirect Reference to Solution - term solution is implied, but negligible.

Direct Reference to Solution - term solution is implied or suggested, but is not explicitly addressed.

Mentions Solution - term is explicitly written within an Article, shows direct evidence of addressing solution.

Results of the Zuboff Rubric: Implicit Solutions to Legitimatize Detection and Sanctions in Business/Consumer Transactions Based on the California Consumer Privacy Act (CCPA)

Government Should Offer Mechanism for Consumers to Report Data Privacy Violations from Businesses — (Explicitly Mentions Solution)

The law "Explicitly Mentions Solution" by permitting consumers to file a complaint with California's Attorney General. Consumers can take civil action against a business if they believe the business has violated their data privacy rights.[166]

"Article 1798.150" states that if consumers' nonencrypted or nonredacted information has been disclosed or stolen from a business, then the business may be held liable under civil action for damages.[167]

Businesses Should Provide Consumers with a Contract for Data Collection, Usage and Sale — (Indirect Reference to Solution)

The law does not mention or reference the need for businesses to provide consumers with a contract for the collection, usage and sale of data. However, the law mandates that businesses inform consumers of any data processing that takes place and its purpose during or before processing occurs. Businesses are also required to allow consumers to opt-out from having their data shared or sold to third parties. Providing

---

[166] "California Consumer Privacy Act (CCPA)."

[167] "California Consumer Privacy Act (CCPA)."

consumers with the ability to opt-out of data shares and sales of data and mandating consumers be provided with processing information offers an "Indirect Reference to Solution" for consumers.[168]

"Article 1798.100" states that a business shall inform consumers of data collection before or during the time of processing. A business must also inform consumers of the categories of data that will be processed, the purposes for using the categories of personal information and the timeframe that the data will be stored.[169]

"Article 1798.120" businesses must provide consumers with the ability to opt-out of having their data shared or sold to third parties. [170]

"Article 1798.135" mandates that businesses must provide consumers an opt-out ability from having their data sold or shared with third parties. An opt-out link that reads "Do Not Sell My Personal Information" must be provided to consumers in a visible place on the business' website.[171]

Businesses Have Company Practices and Guidelines Available to Consumers (data: collection, algorithms, sales, experimentations, location and timeframe of storage) — (Indirect Reference to Solution)

The law provides an "Indirect Reference to Solution". It requires businesses to provide consumers with information pertaining to the data that will be processed. This

---

[168] "California Consumer Privacy Act (CCPA)."

[169] "California Consumer Privacy Act (CCPA)."

[170] "California Consumer Privacy Act (CCPA)."

[171] "California Consumer Privacy Act (CCPA)."

information includes whether or not the data will be sold or shared with third parties and the categories of third parties, the timeframe the data will be stored and the categories of data to be processed. It is not expected for businesses to inform consumers where the processed data will be stored, if the data processed will be used for algorithm development or if experiments will be performed on the data.[172]

"Article 1798.100" gives consumers the right to request information from businesses on the details of the data processed. Businesses must inform consumers of the purpose of data collection, data collection categories, sources from where the personal information is collected from and categories of third parties that will receive the data. Consumers must be informed before or during the time of processing.[173]

"Article 1798.110" allows consumers to request a report on the data processed; however, that request does not include details on algorithms, experimentations and storage location information.

"Article 1798.115" has the right to request a report from businesses that sell or share data with third parties. This report holds the same expectations as in "Article 1798.110".[174]

Businesses Provide Consumers with Easy to Understand Contracts — (Indirect Reference to Solution)

Contracts for the collection of data are not references or mentioned within the law. However, consumers are given the right to opt-out of having their data sold or shared to

[172] "California Consumer Privacy Act (CCPA)."

[173] "California Consumer Privacy Act (CCPA)."

[174] "California Consumer Privacy Act (CCPA)."

third parties, which businesses must provide through an easy-to-understand and clearly marked link on the business' website. The link must read "Do Not Sell or Share My Personal Information".[175]

"Article 1798.135" requires businesses to provide a clear and visible link for consumers to opt-out of having their data sold. This link should be titled "Do Not Sell or Share My Personal Information" and placed in a visible location on the businesses' website.[176]

Government Enforcement of Hefty Fines or Suspension of Service and Order Deletion of Unauthorized Consumer Data when Businesses Violate Data Privacy Rules for Consumers — (Direct Reference to Solution)

The law offers a "Direct Reference to Solution" where the court may order businesses to pay a fine in order to alleviate any damages done to consumers' data, that is, if the court finds that a business is responsible for the disclosure or theft of consumers' nonencrypted or nonredacted data. The law does not mention or reference suspending businesses' services if found guilty of violating data privacy practices. However, the business must comply with any relief deemed reasonable by the court.[177]

"Article 1798.150" allows for consumers to file a civil action suit against a business in order to recover damages. The maximum fine permitted cannot exceed $750 per consumer per incident. If the business faces a class-wide action, then the business is

[175] "California Consumer Privacy Act (CCPA)."

[176] "California Consumer Privacy Act (CCPA)."

[177] "California Consumer Privacy Act (CCPA)."

allotted 30 days to rectify the situation and if the issue is solved, no further action shall take place.[178]

Under "Article 1798.155," the California Attorney General can take further actions if a business or third party fails to cure any alleged violation. The civil penalty can result in a fine ranging between $2500 to $7500. Once collected, the fine will go to the Consumer Privacy Fund.[179]

Summary of the Zuboff Rubric: Results and Observations of the GDPR and CCPA

After analyzing and comparing the GDPR and CCPA to the concerns of the Zuboff Rubric, it is apparent that both laws can provide consumers a level of data privacy protection. However, the GDPR addresses more solutions than the CCPA. Out of the twelve listed solution items between the two sections of the Zuboff Rubric, the GDPR addresses "Explicitly Addresses Solution" five times, "Direct Reference to Solution" five times, "Indirect Reference to Solution" zero times and "Clearly Absent of Solution" two times. While the CCPA addresses "Explicitly Addresses Solution" two times, "Direct Reference to Solution" three times, "Indirect Reference to Solution" five times and "Clearly Absent of Solution" two times. Based on the Zuboff Rubric results, the GDPR is better equipped than the CCPA is at addressing Zuboff's concerns and, therefore, is better equipped to provide data privacy protections for consumers.

---

[178] "California Consumer Privacy Act (CCPA)."

[179] "California Consumer Privacy Act (CCPA)."

When providing consumer data privacy protections, the GDPR and CCPA offer some similarities but many more differences. For example, under both laws, consumers are permitted to request a report from businesses pertaining to information about their data processed, have their data deleted from the business' databases and file a complaint once a business has violated their data protection as provided by the laws. However, the differences are much more vast, showing that the GDPR offers greater data privacy protections.

One major difference revealed after a complete overview of Zuboff Rubric is that the GDPR serves as a proactive law in protecting data privacy, while the CCPA is a reactionary law. The GDPR provides consumers a barrier of protection before businesses are permitted to process data. Businesses must have an explicit reason that is legally admissible and an action plan for keeping data secure before being permitted to process consumer data. Additionally, if consumers still have concerns over their data or wish not to have their data processed, consumers can deny businesses from processing data. The CCPA does not have specific criteria for businesses to process consumer data, nor do consumers have the authority to deny data processing.

Another notable distinction between the laws is that the CCPA addresses similar issues to the GDPR but at a limited capacity. The CCPA does not allow consumers to deny data collection like the GDPR but does require businesses to provide consumers with the choice of opting out of data sharing or selling to third parties. Both laws mandate that businesses provide consumers with data processing information at or before the time of processing, but the CCPA requires fewer details.

Under these two laws, businesses must inform consumers of when data is process, the timeframe the data will be stored, the purpose for processing the data, if the data will be shared or sold, and the categories of third parties to receive the data. However, the GDPR also requires businesses to provide a legal basis for the act processing, contact details of the data processor and third-party vendors, safeguards put into place when businesses sell data to third-party countries and any existence of automated decision-making or profiling resulting from the data process.

If a business is found guilty of violating data privacy regulations set by either of these laws, consumers can seek retribution of damages where the business can face a fine. The GDPR can fine businesses, depending on the violation, 10,000,000 Euros or 2 percent of the business' worldwide annual income if the business was unaware of the offense or 2,000,000 Euros or 4 percent annual income if the business knew about the offense.[180] Businesses that violate consumers' privacy rights under the CCPA and are found guilty can be fined anywhere between $100 or $750 per consumer per incident of a security breach. A business that violates the law may face an administrative fine of $2500 for each violation or $7500 for each violation that is found to be intentional. Businesses that violate the GDPR are potentially faced with much steeper fines.[181]

It should also be mentioned that under the CCPA, the only businesses that are held liable are ones that have an annual gross revenue higher than $25,000,000, buys, sells, or shares the data of 100,000 consumers or the business' annual revenues derived from

---

[180] "General Data Protection Regulation (GDPR)."

[181] "California Consumer Privacy Act (CCPA)."

selling or sharing fifty percent or more of consumers' data. Nonprofits do not qualify. Unlike the CCPA, any entity that processes data is liable to comply with the GDPR.[182]

The GDPR may address more concerns than the CCPA, but both laws still have room for improvement. As discovered through the Zuboff Rubric, neither law provides consumers with the authority of deciding with whom specifically they share their data, nor requires a contract between consumer and business for data processing and does not provide a full account of information of the data process itself. The laws do not enforce an alternative method to data collection, (i.e., offering consumers paid access to the website where no data will be collected).

Thus, as discovered through the Zuboff Rubric, neither law provides consumers with complete autonomy over their data. Currently, businesses have considerable control over consumers data, more than consumers are aware. Through the GDPR and CCPA, consumers are provided with some control over how their data is handled. However, the GDPR based on the Zuboff Rubrics is better equipped at providing consumers data privacy protections.

---

[182] "California Consumer Privacy Act (CCPA)."

Chapter V.

Conclusion and Reflections

Varian, Zuboff and others have discussed the benefits and disadvantages of data collection. With the aggregation of data, businesses can provide consumers with a customized experience. Consumers can enjoy tailored news, music, directions, purchases and much more based on their preferences that are determined by algorithms experimenting with their data. The experience can be pleasurable, but consumers are often unaware that information about their identity and habits is being collected and experimented on to create that experience.

As Zuboff explains, the biggest dangers of data collection are consumers' lack of knowledge on data processing and the limited amount of control consumers have over their data.[183] Since the origin of the internet, businesses have been the sole regulator of consumer data. Businesses have set the standards on what type of data is collected, how much of it will be processed and when.[184] To ensure businesses are providing safety measurements for consumers when processing their data, checks and balances need to be put into place. Government regulation of data control can protect consumers from unsafe or unwanted data collection. The GDPR (2018) and the CCPA (2020) were both enacted to protect the data of EU and California residents. Although fairly new, each law can provide innovative solutions to data access control.

---

[183] Zuboff, "Big Other," 75-89.

[184] West, "Data Capitalism," 25-27.

This thesis aimed to determine which law is better equipped at providing data protection for consumers by using Zuboff's list of concerns to develop a dual rubric of legal effectiveness titled Implicit Solutions for Current Asymmetries of Knowledge and Power in Business/Consumer Transactions and Implicit Solutions to Legitimatize Detection and Sanctions in Business/Consumer Transactions. Results of the Rubrics determined that the GDPR is better equipped to address Zuboff's concerns and provide data privacy protections for consumers and that it is proactive in protecting consumer data privacy, whereas the CCPA is reactive. Thus, this test offered insight into how well each law can protect consumer data and expose areas that need improvement.

The results of the Zuboff Rubric present opportunities to improve data privacy laws as the internet and how we interact with it continuously evolve. During the 2020 pandemic, businesses and consumers, employers and employees, schools and students were forced to utilize the internet in unimaginable ways. The accelerated development propelled the use of technology years ahead of its time. Perhaps the severity of the pandemic blanketed any prior fears we had of the internet and allowed us to invite this unexpected guest into our homes without asking the proper questions.

We must now look forward and question how much of our data is living freely in cyberspace and how does it affect us? One thing is known, the amount of information produced continues to increase each year, as does the number of devices connected to the internet. This information we willingly or unwillingly provide cannot be deleted or returned as we do not understand where it has gone, and for some, cannot comprehend its existence. The best way to protect consumers is by regulating data extraction.

The US legal system is beginning to catch on to the importance of protection against technology by creating laws to protect data privacy. Aside from California developing a state-wide data privacy act, the Obama administration developed the Consumer Privacy Bill of Rights in 2012. This Bill has been considered the blueprint for the development of a federal data privacy law but has yet to be used in federal legislation.[185] Following this bill, the Information Transparency and Personal Data Control Act was introduced to the House in 2019[186] and the Consumer Data Privacy and Security Act of 2020 was introduced to the Senate in March of 2020.[187] Both Bills have yet to be approved but would provide extensive data privacy regulations for the US.

Without a federal data privacy law, several states have decided to develop state-wide protections for their residents. During the 2021 State of the State proposal in New York, Governor Andrew Cuomo proposed a law that would mandate companies to be transparent about the types of data collected and the purpose for data collection of all New York residents. The proposed bill called the Consumer Data Privacy Bill of Rights, would provide New York residents the right to request the deletion of personal data from business records, grant access and control over one's own data and not be faced with

---

[185] Cameron F. Kerry, "Why Protecting Privacy Is a Losing Game Today-and How to Change the Game," Brookings, October 25, 2019, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

[186] Suzan K. DelBene, "Text - H.R.2013 - 116th Congress (2019-2020): Information Transparency & Personal Data Control Act," Congress.gov, April 2, 2019, https://www.congress.gov/bill/116th-congress/house-bill/2013/text.

[187] Jerry Moran, "Text - S.3456 - 116th Congress (2019-2020): Consumer Data Privacy and Security Act of 2020," Congress.gov, March 12, 2020, https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

discrimination for exercising these rights. This bill will incorporate articles from both the GDPR and the CCPA and is expected to be one of the most comprehensive data privacy bills in the nation, surpassing the CCPA. To ensure the success of the law, New York is expected to work closely with other states.[188] However, if the state-by-state implementation of data privacy laws continues, fifty states (plus territories) may provide just as many data privacy laws causing potential confusion across the country. Federal regulation would prevent such complications and would create an opportunity for the US to be a pioneer in the global protection of online securities.

The EU has begun taking the stage of enforcing global data privacy protections for their residents, which is not surprising given the history of the EU's privacy protections. The EU's data privacy model is quickly setting the standard for data privacy laws globally and does not plan on slowing down.[189] Proposed in December 2020, the Digital Services Act (DSA) aims to change the way internet firms conducts business with consumers by expanding liability, competition and employment criteria to further enhance privacy rights online.[190] The EU is proactive in protecting its residents from

---

[188] "Governor Cuomo Announces Proposal to Safeguard Data Security Rights as Part of the 2021 State of the State," (January 21, 2020): governor.ny.gov, https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-safeguard-data-security-rights-part-2021-state-state.

[189] Michael L. Rustad and Thomas H. Koenig, "Towards a Global Data Privacy Standard," *Florida Law Review* 71 (2019): 365-453.

[190] Aline Blankertz and Julian Jaursch, "How the EU plans to rewrite the rules for the internet," *Brookings* (October 21, 2020): https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet/.

potential harms of the internet, which is quickly becoming as essential as the need for water.

As technology continues to develop, society faces many more dangers, such as cyber hacking and cyber warfare. However, with more internet regulations worldwide, online interactions can become safer for users within the globally unregulated space. Until governments implement regulations that coincides with the ever-developing technology market, it is imperative that consumers are informed of the actions businesses perform behind the scenes as well as the services they provided. Only then can consumers truly have the power to protect themselves and hold businesses and governments accountable to provide proper data privacy protections. Being informed and taking back ownership of our data will help set the trajectory of online operations. Governments should take action like the EU has in creating online safety nets for their residents.

The internet itself may never be entirely secure, but data privacy laws can help provide protections for its users. Varian and Zuboff may never agree on the level of interaction businesses have with their consumers as they argued the benefits and disadvantages of data collection. However, they both can agree on one thing that internet-connected, computer-mediated transactions will continue to be employed by consumers and businesses for the foreseeable future, and I think we can all agree.

Appendix 1.

GDPR[191]

Art. 6 GDPR Lawfulness of processing

Processing shall be lawful only if and to the extent that at least one of the following applies: the data subject has given consent to the processing of his or her personal data for one or more specific purposes; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with a legal obligation to which the controller is subject; processing is necessary in order to protect the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

---

[191] "GDPR Archives," GDPR.eu, accessed May 1, 2021, https://gdpr.eu/tag/gdpr/.

Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

Union law; or

Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. 4The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member

State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10; the possible consequences of the intended further processing for data subjects; the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Art. 7 GDPR Conditions for consent

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent

before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject

The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one

month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

Art. 13 GDPR Information to be provided where personal data are collected from the data subject

Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: the identity and the contact details of the controller and, where applicable, of the controller's representative; the contact details of the data protection officer, where applicable; the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if any; where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following

further information necessary to ensure fair and transparent processing: the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2

Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Art. 15 GDPR Right of access by the data subject

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; the right to lodge a complaint with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source; the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request

by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Art. 17 GDPR Right to erasure ('right to be forgotten')

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the

data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or for the establishment, exercise or defence of legal claims.

Art. 18 GDPR Right to restriction of processing

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; the data subject

has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

Art. 21 GDPR Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Art. 22 GDPR Automated individual decision-making, including profiling

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Paragraph 1 shall not apply if the decision: is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent.

In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Art. 77 GDPR Right to lodge a complaint with a supervisory authority

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.

The supervisory authority with which the complaint has been lodged shall inform the complainant on the progress and the outcome of the complaint including the possibility of a judicial remedy pursuant to Article 78.

Art. 79 GDPR Right to an effective judicial remedy against a controller or processor

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article

77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Article 82 Right to compensation and liability

1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

3. A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

4. Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor

shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

5. Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.4.5.2016 EN Official Journal of the European Union L 119/81

6. Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Article 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of

data subjects affected and the level of damage suffered by them; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial

year, whichever is higher: (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; (b) the obligations of the certification body pursuant to Articles 42 and 43; (c) the obligations of the monitoring body pursuant to Article 41(4). L 119/82 EN Official Journal of the European Union 4.5.2016

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher: (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9; (b) the data subjects' rights pursuant to Articles 12 to 22; (c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49; (d) any obligations pursuant to Member State law adopted under Chapter IX; (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive.

Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

Art. 84 GDPR Penalties

Member States shall lay down the rules on other penalties applicable to infringements of this Regulation in particular for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. Such penalties shall be effective, proportionate and dissuasive.

Each Member State shall notify to the Commission the provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them.

Appendix 2.

CCPA[192]

Article 1798.100.

(a) A consumer shall have the right to request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing consumers with notice consistent with this section.

(c) A business shall provide the information specified in subdivision (a) to a consumer only upon receipt of a verifiable consumer request.

(d) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to consumers, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, readily useable format that allows consumers to transmit this information to another entity without hindrance. A

---

[192] "California Consumer Privacy Act (CCPA)."

business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.

Article 1798.105.

(a) A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.

(b) A business that collects personal information about consumers shall disclose, pursuant to Section 1798.130, the consumer's rights to request the deletion of the consumer's personal information.

(c) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information pursuant to subdivision (a) of this section shall delete the consumer's personal information from its records and direct any service providers to delete the consumer's personal information from their records.

(d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:

(1) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

(2) Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

(3) Debug to identify and repair errors that impair existing intended functionality.

(4) Exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law.

(5) Comply with the California Electronic Communications Privacy Act pursuant to Chapter 3.6 (commencing with Section 1546) of Title 12 of Part 2 of the Penal Code.

(6) Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the business' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

(7) To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

(8) Comply with a legal obligation.

(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

Article 1798.110.

(a) A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following:

(1) The categories of personal information it has collected about that consumer.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information. (4) The categories of third parties with whom the business shares personal information. (5) The specific pieces of personal information it has collected about that consumer.

(b) A business that collects personal information about a consumer shall disclose to the consumer, pursuant to paragraph (3) of subdivision (a) of Section 1798.130, the information specified in subdivision (a) upon receipt of a verifiable consumer request from the consumer.

(c) A business that collects personal information about consumers shall disclose, pursuant to subparagraph (B) of paragraph (5) of subdivision (a) of Section 1798.130:

(1) The categories of personal information it has collected about consumers.

(2) The categories of sources from which the personal information is collected.

(3) The business or commercial purpose for collecting or selling personal information.

(4) The categories of third parties with whom the business shares personal information.

(5) That a consumer has the right to request the specific pieces of personal information the business has collected about that consumer.

Article 1798.115.

(a)Aconsumershallhavetherighttorequestthatabusinessthatsellstheconsumer'spersonal information, or that discloses it for a business purpose, disclose to that consumer:

(1) The categories of personal information that the business collected about the consumer.

(2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each category of third parties to whom the personal information was sold.

(3) The categories of personal information that the business disclosed about the consumer for a business purpose.

Article 1798.120.

(a)A consumer shall have the right, at anytime, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.

(b) A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information.

(c) Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers at least 13 years of age and less than 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information. A business that willfully disregards the consumer's age

shall be deemed to have had actual knowledge of the consumer's age. This right may be referred to as the "right to opt-in."

Article 1798.130.

(a) In order to comply with Sections1798.100,1798.105,1798.110,1798.115,and1798.125,a business shall, in a form that is reasonably accessible to consumers:

(1) (A) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number. A business that operates exclusively online and has a direct relationship with a consumer from whom it collects personal information shall only be required to provide an email address for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(B) If the business maintains an internet website, make the internet website available to consumers to submit requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115.

(2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable consumer request from the consumer. The business shall promptly take steps to determine whether the request is a verifiable consumer request, but this shall not extend the business' duty to disclose and deliver the information within 45 days of receipt of the consumer's request. The time period to provide the required information may be extended once by an additional 45 days when

reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period. The disclosure shall cover the 12-month period preceding the business' receipt of the verifiable consumer request and shall be made in writing and delivered through the consumer's account with the business, if the consumer maintains an account with the business, or by mail or electronically at the consumer's option if the consumer does not maintain an account with the business, in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance. The business may require authentication of the consumer that is reasonable in light of the nature of the personal information requested, but shall not require the consumer to create an account with the business in order to make a verifiable consumer request. If the consumer maintains an account with the business, the business may require the consumer to submit the request through that account.

(3) For purposes of subdivision (b) of Section 1798.110:

(A) To identify the consumer, associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information collected about the consumer in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information collected.

(4) For purposes of subdivision (b) of Section 1798.115:

(A) Identify the consumer and associate the information provided by the consumer in the verifiable consumer request to any personal information previously collected by the business about the consumer.

(B) Identify by category or categories the personal information of the consumer that the business sold in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was sold in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information sold. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (C).

(C) Identify by category or categories the personal information of the consumer that the business disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information, and provide the categories of third parties to whom the consumer's personal information was disclosed for a business purpose in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describes the personal information disclosed. The business shall disclose the information in a list that is separate from a list generated for the purposes of subparagraph (B).

(5) Disclose the following information in its online privacy policy or policies if the business has an online privacy policy or policies and in any California-specific description of consumers' privacy rights, or if the business does not maintain those

policies, on its internet website and update that information at least once every 12 months:

(A) A description of a consumer's rights pursuant to Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125 and one or more designated methods for submitting requests.

(B) For purposes of subdivision (c) of Section 1798.110, a list of the categories of personal information it has collected about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information collected.

(C) For purposes of paragraphs (1) and (2) of subdivision (c) of Section 1798.115, two separate lists:

(i) A list of the categories of personal information it has sold about consumers in the preceding 12 months by reference to the enumerated category or categories in subdivision (c) that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact.

(ii) A list of the categories of personal information it has disclosed about consumers for a business purpose in the preceding 12 months by reference to the enumerated category in subdivision (c) that most closely describe the personal information disclosed, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

(D) In the case of a business that sells or discloses deidentified patient information not subject to this title pursuant to clause (i) of subparagraph (A) of paragraph (4) of subdivision (a) of Section 1798.146, whether the business sells or discloses deidentified patient information derived from patient information and if so, whether that patient information was deidentified pursuant to one or more of the following:

(i) The deidentification methodology described in Section 164.514(b)(1) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA expert determination method.

(ii) The deidentification methodology described in Section 164.514(b)(2) of Title 45 of the Code of Federal Regulations, commonly known as the HIPAA safe harbor method.

(6) Ensure that all individuals responsible for handling consumer inquiries about the business' privacy practices or the business' compliance with this title are informed of all requirements in Sections 1798.100, 1798.105, 1798.110, 1798.115, and 1798.125, and this section, and how to direct consumers to exercise their rights under those sections.

(7) Use any personal information collected from the consumer in connection with the business' verification of the consumer's request solely for the purposes of verification.

(b) A business is not obligated to provide the information required by Sections 1798.110 and 1798.115 to the same consumer more than twice in a 12-month period.

(c) The categories of personal information required to be disclosed pursuant to Sections 1798.110 and 1798.115 shall follow the definition of personal information in Section 1798.140.

Article 1798.135.

(a)A business that is required to comply with Section1798.120 shall, inform that is reasonably accessible to consumers:

(1) Provide a clear and conspicuous link on the business's Internet homepage, titled "Do Not Sell My Personal Information," to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt-out of the sale of the consumer's personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer's personal information.

(2) Include a description of a consumer's rights pursuant to Section 1798.120, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in:

(A) Its online privacy policy or policies if the business has an online privacy policy or policies.

(B) Any California-specific description of consumers' privacy rights.

(3) Ensure that all individuals responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with this title are informed of all requirements in Section 1798.120 and this section and how to direct consumers to exercise their rights under those sections.

(4) For consumers who exercise their right to opt-out of the sale of their personal information, refrain from selling personal information collected by the business about the consumer.

(5) For a consumer who has opted-out of the sale of the consumer's personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information.

(6) Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) Nothing in this title shall be construed to require a business to comply with the title by including the required links and text on the homepage that the business makes available to the public generally, if the business maintains a separate and additional homepage that is dedicated to California consumers and that includes the required links and text, and the business takes reasonable steps to ensure that California consumers are directed to the homepage for California consumers and not the homepage made available to the public generally.

(c) A consumer may authorize another person solely to opt-out of the sale of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to regulations adopted by the Attorney General.

(Amended (as added by Stats. 2018, Ch. 55, Sec. 3) by Stats. 2018, Ch. 735, Sec. 8. (SB 1121) Effective September 23, 2018. Section operative January 1, 2020, pursuant to Section 1798.198.)

Article 1798.150.

(a)(1) Any consumer whose non encrypted and non redacted personal information,as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

(2) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth.

(b) Actions pursuant to this section may be brought by a consumer if, prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated. In

the event a cure is possible, if within the 30 days the business actually cures the noticed violation and provides the consumer an express written statement that the violations have been cured and that no further violations shall occur, no action for individual statutory damages or class-wide statutory damages may be initiated against the business. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations of this title. If a business continues to violate this title in breach of the express written statement provided to the consumer under this section, the consumer may initiate an action against the business to enforce the written statement and may pursue statutory damages for each breach of the express written statement, as well as any other violation of the title that postdates the written statement.

Article 1798.155.

(a)Any business or third party may seek the opinion of the Attorney Generalfor guidance on how to comply with the provisions of this title.

(b) A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation, which shall be assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General. The civil penalties provided

for in this section shall be exclusively assessed and recovered in a civil action brought in the name of the people of the State of California by the Attorney General.

(c) Any civil penalty assessed for a violation of this title, and the proceeds of any settlement of an action brought pursuant to subdivision (b), shall be deposited in the Consumer Privacy Fund, created within the General Fund pursuant to subdivision (a) of Section 1798.160 with the intent to fully offset any costs incurred by the state courts and the Attorney General in connection with this title.

Bibliography

"The Bill of Rights: What Does It Say?" National Archives. The U.S. National Archives and Records Administration. Last reviewed July 24, 2020. https: www.archives.gov/founding-docs/bill-of-rights/what-does-it-say.

Blankertz, Aline and Julian Jaursch. "How the EU plans to rewrite the rules for the internet." Brookings (October 21, 2020): https://www.brookings.edu/techstream/how-the-eu-plans-to-rewrite-the-rules-for-the-internet/.

"California Consumer Privacy Act (CCPA)." State of California Department of Justice. Office of the Attorney General. Accessed March 3, 2021. https://www.oag.ca.gov/privacy/ccpa.

Colburn, Ken. "Computer cookies: What they are and how to manage them." *Microsoft News*, (October 19, 2020): https://www.msn.com/en-us/news/technology/computer-cookies-what-they-are-and-how-to-manage-them/ar-BB1aaQWH.

"Convention for the Protection of Human Rights and the Fundamental Freedoms." European Convention on Human Rights. European Court of Human Right. (Accessed 2021): https://www.echr.coe.int/Documents/Convention_ENG.pdf.

DelBene, Suzan K. "Text - H.R.2013 - 116th Congress (2019-2020): Information Transparency and Personal Data Control Act." *Congress.Gov*. (April 2, 2019): https://www.congress.gov/bill/116th-congress/house-bill/2013/text.

"Directive 2006/24/EC of the European Parliament and of The Council of 15 March 2006." EUR-Lex Access to the European Union law. Publications Office of the European Union. (Accessed 2021): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0024.

Eberle, Edward J. "The Methodology of Comparative Law." *Roger Williams University Law Review* 16, Iss. 1 (2011): 51-72. http://docs.rwu.edu/rwu_LR/vol16/iss1/2.

"The History of the General Data Protection Regulation." European Data Protection Supervisor. (Accessed 2021): https://edps.europa.eu/data-protection/our-work/publications/legislation/council-europe-convention-no-108-data-protection_en.

"Gramm-Leach-Bliley Act." Federal Trade Commission. (Accessed 2021): https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

Freed Wessler, Nathan. "The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In." ACLU Massachusetts. July 1, 2019. https://www.aclum.org/en/publications/supreme-courts-most-consequential-ruling-privacy-digital-age-one-year.

"General Data Protection Regulation." GDPR.eu. (Accessed 2021): https://gdpr.eu/tag/gdpr/.

"Governor Cuomo Announces Proposal to Safeguard Data Security Rights as Part of the 2021 State of the State." The Official Website of New York State. New York State. (Accessed 2021): https://www.governor.ny.gov/news/governor-cuomo-announces-proposal-safeguard-data-security-rights-part-2021-state-state.

"Gramm-Leach-Bliley Act." Federal Trade Commission Protecting America's Consumers. (Accessed 2021): https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

"Google Spain SL V. agencia española de protección de datos." *Harvard Law Review*, (December 10, 2014). https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/.

"The History of the General Data Protection Regulation." European Data Protection Supervisor. (Accessed 2021): https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

Klebnikov, Sergei. "Google Parent Alphabet Passes $1 Trillion in Market Value." *Forbes*, (January 13, 2020): https://www.forbes.com/sites/sergeiklebnikov/2020/01/13/google-parent-alphabet-set-to-hit-1-trillion-in-market-value/?sh=190b55a14dcf.

Kerry, Cameron F. "Why Protecting Privacy Is a Losing Game Today-and How to Change the Game." *Brookings,* (October 25, 2019): https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

Lange, Christian. "Noble Lecture." The Nobel Prize. Nobel Prize Outreach AB 2021. (Accessed 2021):https://www.nobelprize.org/prizes/peace/1921/lange/lecture/.

McAfee, Andrew and Erik Brynjolfsson. "Big Data: The Management Revolution."

Harvard Business Review. (October 8, 2014): https://hbr.org/2012/10/big-data-the-management-revolution.

Moran, Jerry "Text - S.3456 Consumer Data Privacy and Security Act of 2020 - 116th Congress (2019-2020)." Congress.Gov. Library of Congress. (March 12, 2020): https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

Nissenbaum, Helen. "A Contextual Approach to Privacy Online." *Daedalus* 140, no. 4 (Fall 2011): 30-48. https://www.amacad.org/sites/default/files/daedalus/downloads/Fa2011_Protecting-the-Internet-as-Public-Commons.pdf.

Rothstein, Mark A. and Stacey A Tovino, "California Takes the Lead on Data Privacy Law," *Hastings Center Report* 49, No. 5 (September 2019): 4-5. https://www.ncbi.nlm.nih.gov/pubmed/31581323.

Rustad, Michael L. and Thomas H. Koenig. "Towards a Global Data Privacy Standard." *Florida Law Review* 71 (2019): 365-453.

Schrodt, Paul. "Edward Snowden Just Made an Impassioned Argument for Why Privacy Is the Most Important Right." Business Insider. Insider Inc. (September 15, 2016): https://www.businessinsider.com/edward-snowden-privacy-argument-2016-9?op=1.

Schwartz, Paul M. "The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures," *Harvard Law Review* 126, no. 7 (May 2013): 1966-2009. https://harvardlawreview.org/2013/05/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/.

Sensenbrenner Jr., Rep. James. F. "H.R.2048 - USA Freedom Act of 2015." Congress.Gov. Library of Congress. (June 2, 2015): https://www.congress.gov/bill/114th-congress/house-bill/2048/

Solove, Daniel J. "A Brief History of Information Privacy Law." *George Washington University Law School*. (2006): 1-46. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2076&context=faculty_publications.

"The Telecommunications (Data Protection and privacy) (Direct Marketing) Regulations 1998," legislaition.gov.uk. Crown and database right. (Accessed 2021): https://www.legislation.gov.uk/uksi/1998/3170/made.

"Universal declaration of human rights." United Nations. United Nations Publications. (Accessed 2021): https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Varian, Hal R. “Beyond Big Data.” *Business Economics* 49 (2014): 27-31. https://link.springer.com/article/10.1057%2Fbe.2014.1.

Waldersee, Victoria. “EU’s Vestager Backs Twitter for Banning Political Ads, Berates Facebook.” *Reuters*. (November 7, 2019): https://www.reuters.com/article/us-eu-antitrust-twitter-facebook-idUSKBN1XH2I2.

Wessler, Nathan Freed. “The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In.” *ACLU Massachusetts*. (July 1, 2019): https://www.aclum.org/en/publications/supreme-courts-most-consequential-ruling-privacy-digital-age-one-year.

West, Sarah Myers. “Data Capitalism: Redefining the Logics of Surveillance and Privacy.” *Business and Society* 58, no. 1 (2019): 20-41. https://journals.sagepub.com/doi/10.1177/0007650317718185.

Wheatley, Alec. “Do-It-Yourself Privacy: The Need for Comprehensive Federal Privacy Legislation with A Private Right of Action.” *Golden Gate University Law Review* 45, no. 3 (September 2015): 265-86. https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=2150&context=ggulrev.

Whitman, James Q. “The Two Western Cultures of Privacy: Dignity Versus Liberty.” *Yale Law Journal* 113, no 6 (April 2004): 1153-1251.

Zuboff, Shoshana. “About” shoshanazuboff.com. (2021), https://shoshanazuboff.com/book/shoshana/.

Zuboff, Shoshana. “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,” *Journal of Information Technology* 30, no. 1 (2015): 75-89. https://journals.sagepub.com/doi/10.1057/jit.2015.5.