University of Dayton Law Review

Volume 45 | Number 1 Article 5

1-1-2020

Big Data, Little Privacy: Protecting Consumers' Data While Promoting Economic Growth

Mary Kraft
University of Dayton

Big Data, Little Privacy: Protecting Consumers' Data While Promoting Economic Growth

Cover Page Footnote

Thank you to my family and friends for their support and encouragement throughout my entire law school experience. Thank you to my Comment Editor, Madison Rittley, for her mentorship, guidance, and wit. Finally, I would like to thank Professor Thaddeus Hoffmeister and Professor Susan Wawrose for their sage advice and direction during the writing process.

BIG DATA, LITTLE PRIVACY: PROTECTING CONSUMERS' DATA WHILE PROMOTING ECONOMIC GROWTH

Mary Kraft[*]

[*] J.D. Candidate (expected 2020) at the University of Dayton School of Law. Thank you to my family and friends for their support and encouragement throughout my entire law school experience. Thank you to my Comment Editor, Madison Rittley, for her mentorship, guidance, and wit. Finally, I would like to thank Professor Thaddeus Hoffmeister and Professor Susan Wawrose for their sage advice and direction during the writing process.

I. INTRODUCTION

"The world's most valuable resource is no longer oil, but data."[1] This multi-billion-dollar industry is led by data brokers, who collect and sell consumer data with minimal oversight, regulation, transparency, and public awareness.[2] First, data is collected, predominantly without consumers' knowledge, from a wide array of both online and offline sources.[3] Collection occurs from examining a consumer's spending habits, memberships with religious and political groups, social media profiles, news and entertainment subscriptions, enrollment in warranty programs, as well as many other aspects of a consumer's everyday life.[4] As data brokers gather information, they analyze the data to make inferences and predictions about individual consumers.[5]

Next, based on their analysis, data brokers place consumers into categories.[6] Consumers would be shocked to learn about the discriminatory and insensitive nature of these category names. In 2014, the Federal Trade Commission ("FTC") studied nine data brokerage firms.[7] Its report revealed

[1] *The World's Most Valuable Resource is No Longer Oil, but Data*, THE ECONOMIST (May 6, 2017), https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

[2] Daniel Wilson, *Rockefeller Wants Light Shined on Data Broker Industry*, LAW360 (Dec. 18, 2013), https://www.law360.com/articles/496763/rockefeller-wants-light-shined-on-data-broker-industry.

[3] Press Release, Fed. Trade Comm'n, FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information (May 27, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

categories such as "Urban Scramble" and "Mobile Mixers," which were used to describe Latino and African-American consumers with low incomes.[8] "Rural Everlasting" was a category referring to consumers who were single, over the age of sixty-six, with minimal education, and low socioeconomic status.[9] Additional examples of problematic category names were "Metro Parents," used to describe indigent single parents with only a high school or vocational education, and "Timeless Traditions," a label depicting immigrants who preferred speaking Spanish but spoke some English.[10] Aside from the appalling category names, the FTC found consumers were treated differently within commercial transactions, depending on the category in which they were placed.[11]

There are three main reasons for buying data: marketing, people searching, and risk mitigation.[12] Companies that buy data for marketing purposes use the information to target ads to consumers.[13] Other data brokers sell personal information via people search websites; companies use these platforms to find public information about consumers and to detect fraud.[14] Finally, in the third category, companies purchase data to mitigate the risk of doing business with a particular consumer.[15]

Risk mitigation brokers allocate risk management scores to individual consumers based on their personal information.[16] Companies use these scores to determine the risk associated with going into business with the particular consumer, or to determine a suitable price to charge the consumer.[17] These scores have been found to correlate with ethnicity, financial status, and the geographical area of where the consumer lives.[18] When a consumer has a score indicating a high level of risk, the company may decline to do business with the consumer or charge the consumer a higher price for the company's services.[19]

However, significant harm can result when inaccurate information

---

[8] *Id.*

[9] *Id.*

[10] Public Statement of Julie Brill, Comm'r of the Fed. Trade Comm'n, on the Comm'n's Report, Data Brokers: A Call for Transparency and Accountability (May 27, 2014), https://www.ftc.gov/system/files/documents/public_statements/311551/140527databrokerrptbrillstmt.pdf.

[11] *Id.*

[12] FTC Press Release, *supra* note 3.

[13] Brian Naylor, *Firms Are Buying, Sharing Your Online Info. What Can You Do About It?*, NPR (July 11, 2016), https://www.npr.org/sections/alltechconsidered/2016/07/11/485571291/firms-are-buying-sharing-your-online-info-what-can-you-do-about-it.

[14] Letter from Jessica Rich, Director of the Fed. Trade Comm'n's Bureau of Consumer Prot., to Nat'l Telecomm. and Info. Admin., Comment: Big Data, Consumer Privacy, and the Consumer Bill of Rights (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573301/140801bigdatacomment.pdf.

[15] FTC Press Release, *supra* note 3.

[16] Public Statement of Julie Brill, *supra* note 10.

[17] *Id.*

[18] *Id.*

[19] *Id.*

incorrectly identifies an individual as a high-risk consumer.[20] For example, what if a bank buys risk mitigation services from a data broker, which it uses to determine whether loan offers will be extended to consumers.[21] Using the service, the bank receives inaccurate information that describes a consumer as a perpetual gambler. The bank declines to go into business with the consumer because the mitigation information described him as being a high-risk. While the consumer knows he has an average credit score and was not expecting to receive the lowest interest rates, he is shocked that the bank flat out denied his loan. He does not know that the bank used risk mitigation products that falsely described him as a perpetual gambler, and therefore he has no way of fixing the error. Because of this inaccurate data, the consumer continues to have difficulty procuring a loan, and when another bank finally accepts his application, he is offered a loan with an astronomical interest rate.

Currently, in the prior scenario, the consumer has incurred actual harm but has no means to identify and correct the untruthful information. The FTC has recommended that Congress enact legislation to make the data broker industry more transparent to consumers and to give consumers more control over the collection and sale of their personal information.[22] Collection and usage of consumer data represents a billion dollar industry in the United States.[23] Just as the Environmental Protection Agency ("EPA") regulates the multi-billion-dollar oil and gas industry, the FTC should be afforded authority to regulate data collection and usage practices.[24] While in the past the United States has been reactive—like in creating the Securities and Exchange Commission ("SEC") to regulate the stock market only after consumers were severely harmed in the market crash of 1929—Congress should be proactive in regulating data collection and usage by vesting the FTC with the power to regulate before a nationwide harm occurs.[25]

The data broker industry is just one way that consumer data is used. According to Dresner Advisory Services' *2017 Big Data Analytics Market Study*, fifty-three percent of companies have adopted big data analytics.[26] Big data analytics are systems that examine "large amounts of data to uncover

---

[20] *Id.*

[21] *See, e.g.*, Raghav Bharadwaj, *Artificial Intelligence for Risk Monitoring in Banking*, FINTECH NEWS (Aug. 30, 2019), https://www.fintechnews.org/artificial-intelligence-for-risk-monitoring-in-banking/ ("Banks and other financial institutions have used [artificial intelligence] in the past for identifying which of their customers might default on credit card payments.").

[22] FTC Press Release, *supra* note 3.

[23] Wilson, *supra* note 2.

[24] *Oil and Gas Sector Information*, U.S. ENVTL. PROT. AGENCY (May 10, 2018), https://www.epa.gov/smartsectors/ oil-and-gas-sector-information.

[25] *Federal Securities Laws*, U.S. SEC. AND EXCH. COMM'N (May 4, 2017), https://www.sec.gov/page/federal-securities-laws?auHash=B8gdTzu6DrpJNvsGIS1-JY1LnXDZQqS-JgJAgaSXimg.

[26] Dresner Advisory Services, *2017 Edition Big Data Analytics Market Study* 12 (Dec. 20, 2017), https://www.microstrategy.com/getmedia/cd052225-be60-49fd-ab1c-4984ebc3cde9/Dresner-Report-Big_Data_Analytic_Market_Study-WisdomofCrowdsSeries-2017.pdf.

hidden patterns, correlations and other insights."[27] Companies can use the contextualized data to improve marketing strategies by understanding how consumers have reacted to previous market campaigns, determining which consumers are most likely to buy their products or services, and predicting what consumers want.[28] Information gained via big data analytics is also used to decrease expenses and improve operational processes.[29]

On the other hand, social media sites (such as Facebook) use consumer data to offer personalized content and features to consumers; to provide security to users; for marketing, research and innovation purposes; and, most importantly, to sell advertisements.[30] However, unlike data brokers, Facebook claims to not sell personally identifiable consumer data to third parties.[31] Instead, the social media site sells advertisement space, and then "provide[s] advertisers with reports about the kinds of people seeing their ads and how their ads are performing."[32] Thus, Facebook offers advertisers general demographic information, rather than specific personally identifiable data.[33] An example of the type of information that Facebook provides to an advertiser is "that an ad was seen by a woman between the ages of [twenty-five] and [thirty-four] who lives in Madrid and likes software engineering."[34]

Just as personal data has affected the way companies perform business, big data has also become utilized in policing and crime investigation.[35] The Los Angeles Police Department's Real-Time Analysis Critical Response Division uses a big data analytics system to create "crime forecasts"—digital maps which predict where crime will occur on any given day.[36] Social media networks represent an additional medium that law enforcement agencies utilize by monitoring suspicious patterns of behavior or activity to predict crimes.[37]

Consumers' information is collected and exploited for a multitude of reasons, and as technology continues to grow, so will the amount of consumer

---

[27] *Big Data Analytics What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/analytics/big-data-analytics.html (last visited Jan. 15, 2020).

[28] Adam C. Uzialko, *How Businesses Are Collecting Data (And What They're Doing with It)*, AGENCY BUS. NEWS DAILY (Aug. 3, 2018), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html.

[29] Randy Bean, *How Companies Say They're Using Big Data*, HARV. BUS. REV. (Apr. 28, 2017), https://hbr.org/2017/04/how-companies-say-theyre-using-big-data%20;%20https://bi-survey.com/big-data-benefits.

[30] *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Jan. 15, 2020).

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] Andrew Ferguson, *The Rise of Big Data Policing*, TECH CRUNCH (Oct. 22, 2017), https://techcrunch.com/2017/10/22/the-rise-of-big-data-policing/.

[36] *Id.*

[37] Lindsey Patterson, *How the Evolution of Big Data is Influencing Law Enforcement*, TECHNOLOGY.ORG (July 28, 2017), https://www.technology.org/2017/07/28/how-the-evolution-of-big-data-is-influencing-law-enforcement/.

data available. While no federal legislation regarding the issue of consumers' data privacy rights exist, on June 28, 2018, California Governor Jerry Brown signed into law The California Consumer Privacy Act of 2018 ("CCPA").[38] The CCPA will be enacted on January 1, 2020, and will have a significant impact on businesses, regardless of their location.[39]

This Comment will demonstrate that a unified, comprehensive federal data privacy statute should be enacted to supersede the CCPA. First, this Comment will provide background regarding how the CCPA became signed into law, and an in-depth description of its content. Second, this Comment will describe the newly enacted European Union's data privacy law, along with other state laws regarding data privacy. Finally, this Comment will explain why a federal regulation should be enacted to supersede state data privacy laws, and suggest the necessary key components of a comprehensive federal data privacy statute.

II. BACKGROUND

A. Putting an amendment on the ballot in California.

In California, citizens may propose constitutional amendments and laws via a ballot initiative.[40] First, the citizen must draft the text of the proposed law, and submit the draft to the Attorney General.[41] To move on in the process, the Attorney General must supply the draft with an official title and summary.[42] Once title and summary are obtained, the citizen must circulate initiative petitions, and collect a requisite number of signatures from registered voters.[43] Upon attainment of a satisfactory amount of signatures, the petition is submitted to "county election officials for verification."[44] Finally, provided the required number of signatures are verified, the initiative will qualify for the ballot, and California voters will vote to approve or deny the initiative.[45] If voters approve the initiative, it will become law.[46]

1. Alastair Mactaggart creates a ballot initiative regarding consumer

---

[38] Kristen J. Mathews & Courtney M. Bowman, *The California Consumer Privacy Act of 2018*, PROSKAUER (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

[39] Emily Tabatabai et al., *Understanding California's Game-Changing Data Protection Law and its Global Impact*, N.Y. L.J. (July 13, 2018, 2:30 PM), https://www.law.com/newyorklawjournal/2018/07/13/071618privacy-389-36894/.

[40] *Ballot Initiatives*, CAL. DEP'T OF JUSTICE, https://oag.ca.gov/initiatives (last visited Jan. 15, 2020).

[41] *Id.*

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *See id.*

data privacy.

Several years before the CCPA was signed into law, Alastair Mactaggart, a successful real estate developer in San Francisco, hosted a dinner party.[47] Among those in attendance was a software engineer at Google.[48] During the party, Mactaggart asked the engineer whether he should be worried about the personal information that Google collects from him.[49] The response to this seemingly lighthearted dinner party satire ignited the spark that would inevitably lead to the enactment of the CCPA: "If people really knew what we had on them, the Google engineer said, they would flip out."[50]

This conversation piqued Mactaggart's interest, and he began researching data mining and privacy policies.[51] To his dismay, he learned these data collectors knew information such as his shoe size, income, and sleeping patterns; but more shockingly, because of all the data collected, these companies could draw sophisticated inferences and make specific predictions about his behavior and conduct.[52] Mactaggart began discussing this data collection issue with Rick Arney, a fellow parent at his son's school.[53] Together, after a year and a half of research, they decided to create a ballot initiative, to give California consumers control over their personal information, centered around three core principles: transparency, control, and accountability.[54]

After six months of drafting, on November 20, 2017, Mactaggart and Arney submitted the final ballot initiative to California.[55] A little over a month later, in January 2018, after receiving a title and summary from the Attorney General of California, Mactaggart and Arney began collecting signatures in preparation to get their initiative on the November 2018 California ballot.[56]

2. Mactaggart's ballot initiative is met by opposition from tech companies.

Mactaggart chaired the Californians for Consumer Privacy, which

---

[47] Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley – and Won*, N.Y. TIMES (Aug. 14, 2018), https://www.nytimes.com/2018/08/14/magazine/facebook-google-privacy-data.html.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Int'l Ass'n of Privacy Prof'ls, *Alastair Mactaggart on the Genesis of the California Consumer Privacy Act of 2018*, YOUTUBE 4:30 (Nov. 14, 2018), https://www.youtube.com/watch?v=kkgn3HtTvjI&feature=em-share_video_user.

[54] *Id.*

[55] *Id.*

[56] *Id.*

spearheaded the campaign in support of the initiative.[57] The campaign raised $3.05 million by June 2018, with 98.4% of the capital donated by Mactaggart himself.[58] The Committee to Protect California Jobs led the campaign in opposition to the initiative and raised $2.15 million by June 2018, receiving contributions from most of the tech giants.[59]

When Mactaggart initially reached out to Facebook looking for support, he did not receive a response.[60] However, once Mactaggart submitted the final draft of the initiative to the Attorney General, officials at Facebook and Google almost immediately contacted Mactaggart and requested to meet in person.[61] Soon afterwards, Mactaggart and Arney met with representatives from Facebook and Google.[62] From these meetings, the tech companies suggested that Mactaggart and Arney pursue legislation, rather than the ballot initiative.[63] Although the pair left their respective meetings feeling positive about a possible collaboration, they soon learned the tech companies "were preparing to crush [them]," and that Facebook and Google had each donated $200,000 to the Committee to Protect California Jobs's campaign in opposition to the initiative.[64]

Just as the opposition campaign began to make waves, news of the now infamous Cambridge Analytica scandal broke, which caused Facebook to bring privacy issues to the forefront of its platform and wide-spread support for Mactaggart's initiative.[65] The initiative ultimately received over 629,000

---

[57] *California Consumer Personal Information Disclosure and Sale Initiative (2018)*, BALLOTPEDIA, https://ballotpedia.org/California_Consumer_Personal_Information_Disclosure_and_Sale_Initiative_(2018) (last visited Jan. 15, 2020).

[58] *Id.*

[59] *Id.* The Committee to Protect California Jobs received donations from: Alliance of Automobile Manufacturers, Inc.; AT&T, Inc. and its Affiliates; California New Car Dealers Associations Issues PAC; Comcast Corporation; Facebook, Inc.; Google, LLC; Verizon Communications, Inc. and its Affiliates; Amazon.com, Inc.; and Microsoft Corporation. *Id.*

[60] *Id.*

[61] Confessore, *supra* note 47.

[62] *Id.*

[63] *Id.*

[64] *Id.*; *California Consumer Personal Information Disclosure and Sale Initiative*, *supra* note 57.

[65] Confessore, *supra* note 47. In June of 2014, an app developer created a personality quiz for Facebook. Around 270,000 Facebook users downloaded the app and took the quiz. However, due to Facebook's policy at the time, the app developer not only gained access to the users' data who took the quiz, but all of their Facebook friends' data as well. Ultimately, the app developer sold over 50 million Facebook users' personal, private information to Cambridge Analytica. Cambridge Analytica, which worked with the Trump 2016 presidential campaign, used this data to spread political content, relating to the election, to voters. Although Facebook learned of the data breach in 2015, the platform did not inform affected users, nor did it discuss the breach with the public, until a *New York Times* story broke news of the scandal in 2018. Robinson Meyer, *The Cambridge Analytica Scandal, in Three Paragraphs*, THE ATLANTIC (Mar. 20, 2018), https://www.theatlantic.com/technology/archive/2018/03/the-cambridge-analytica-scandal-in-three-paragraphs/556046/. After news of the Cambridge Analytica scandal broke in 2018, the FTC launched a year-long investigation of Facebook. Mike Snider & Edward C. Baig, *Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures*, USA TODAY (July 24, 2019, 8:54 AM), https://www.usatoday.com/story/tech/news/2019/07/24/facebook-pay-record-5-billion-fine-u-s-privacy-violations/1812499001/. Ultimately, Facebook accepted a settlement agreement with the FTC in July 2019. *Id.* Under the terms of the settlement, Facebook was required to pay a $5 billion fine, expand its privacy protections, adopt a corporate system to remain in compliance with its newly expanded privacy

verified signatures, almost double the required amount needed to secure a spot on the November 2018 general election ballot.[66]

3. Mactaggart withdraws the ballot initiative on the condition that California legislators pass the CCPA.

In May 2018, after the initiative obtained enough signatures to officially appear on the ballot, Mactaggart had until 5:00 p.m. on June 28, 2018, to withdraw the initiative.[67] The State of California offers the option to withdraw to leave room for legislators to negotiate a deal and propose legislation in lieu of the initiative appearing on the ballot.[68] Legislators wanted to pass the CCPA through the legislative process, rather than taking the chance of it passing through the ballot initiative, because the process of amending a voter-enacted law is exceedingly more difficult.[69] Thus, in May 2018, Assembly member Ed Chau and Senator Bob Hertzberg began reaching out to Mactaggart in hopes of negotiating a deal.[70] "Mactaggart was willing to compromise."[71] Unfortunately, the negotiations started out rocky, as Mactaggart believed the first few drafts of the proposed bill from Hertzberg were meaningless, because they had no enforcement for business accountability.[72]

However, just eight days before the deadline to withdraw, Mactaggart crafted a deal with Chau and Hertzberg.[73] Next, Mactaggart spent the weekend negotiating the bill with various California politicians.[74] The tech companies were the last to jump on board.[75] When faced with an ultimatum, either agree to the legislative deal or continue efforts in opposition through an expensive and unpopular campaign—risking the chance the ballot initiative would be approved by voters—the tech companies ultimately indorsed the deal, and the bill was finalized.[76] Due to California law, which requires the legislature to wait seventy-two hours between writing a bill and voting on it, the bill could not be voted on until 10:47 a.m. on June 28th, just six hours and thirteen minutes before the deadline to withdraw.[77] Ultimately, the bill passed unanimously out of both houses, and Governor Brown signed the CCPA into

---

protections, and maintain a data security program. *Id.* To date, the $5 billion fine is "the largest penalty ever imposed on a company for violating consumers' privacy rights." *Id.*

[66] Mathews & Bowman, *supra* note 38.

[67] Int'l Ass'n of Privacy Prof'ls, *supra* note 53, at 10:00.

[68] *Id.* at 10:00–15:00.

[69] Delilah L. Clay, *California Legislature Cleans Up Privacy Law, But What Next?*, MANATT (Sept. 13, 2018), https://www.manatt.com/insights/newsletters/financial-services-law/california-legislature-cleans-up-privacy-law.

[70] Int'l Ass'n of Privacy Prof'ls, *supra* note 53, at 10:00–15:00.

[71] Confessore, *supra* note 47.

[72] Int'l Ass'n of Privacy Prof'ls, *supra* note 53, at 10:00–15:00.

[73] *Id.*

[74] *Id.*

[75] *See* Confessore, *supra* note 47.

[76] *Id.*; *see generally* Int'l Ass'n of Privacy Prof'ls, *supra* note 53.

[77] Int'l Ass'n of Privacy Prof'ls, *supra* note 53, at 4:30.

law on June 28, 2018.[78]

B. Summary of the CCPA.

1. Consumer rights protected by the CCPA.

The CCPA was enacted for the purpose of establishing transparency in data practices and giving California consumers control over their personal information.[79] The CCPA grants consumers the right: "to know what personal information is being collected about them"; "to know whether their personal information is sold or disclosed and to whom"; "to say no to the sale of personal information"; "to access their personal information"; and "to equal service and price, even if they exercise their privacy rights."[80]

Furthermore, upon a verified request, businesses must disclose the categories of personal information collected about the consumer, the purpose of the category of information, and how the category of information is used.[81] Once a business receives a verified request, it must promptly disclose the information, free of charge, to the consumer.[82] Moreover, while a consumer may request disclosure of his or her personal information at any time, under the CCPA a business need only provide each individual consumer with his or her personal information twice every twelve months.[83]

Additionally, under this law, consumers are given the right to request that a business delete his or her personal information.[84] When this occurs, the business must delete the requested information and direct any service providers, who also have the information, to delete it as well.[85] Consumers also now have the right to "opt-out," thereby prohibiting a business from selling his or her personal information to a third party.[86] Further, the CCPA provides that a third party, who has bought personal information from a business, may not sell the personal information unless the consumer has received notice and an opportunity to opt-out.[87]

The CCPA protects minors by requiring that consumers, aged sixteen years or younger, must "opt-in" by affirmatively authorizing a business to sell their personal information.[88] Consumers between thirteen and sixteen years

---

[78] *Id.*

[79] *See* Assemb. B. 375, 2017-18 Reg. Sess., § 2 (Cal. 2018) (enacted). "'Personal information' means information that identifies, relates to, describes, references, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* § 1798.140(o)(1).

[80] *Id.* § 2 (i)(1)–(5).

[81] *See generally id.* § 1798.100(a)–(d).

[82] *Id.* § 1798.100(d).

[83] *Id.*

[84] *Id.* § 1798.105(a), (c).

[85] *Id.*

[86] *Id.* § 1798.120(a).

[87] *Id.* § 1798.115(d).

[88] *Id.* § 1798.120(d).

old may opt-in themselves, while consumers under the age of thirteen must be opted-in by their parent or guardian.[89] A business violates this provision if it has actual knowledge, or willfully disregards, that the consumer is sixteen years old or younger and has not opted-in.[90]

2. Businesses' obligations under the CCPA.

A "business" under the CCPA is one that does business in California and satisfies at least one of the following thresholds: (1) has an annual gross revenue of more than $25 million; (2) "annually buys, receives for the business' commercial purpose, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices"; or (3) "[d]erives [fifty] percent or more of its annual revenues from selling consumers' personal information."[91]

Furthermore, a business must offer at least two ways for consumers to request disclosure of their personal information: a toll-free number and a website address.[92] Once the business receives a request, it has forty-five days to provide the consumer with the personal information it has collected and sold about him or her within the past twelve months.[93] However, when reasonably necessary, the business may be granted a one-time, forty-five-day extension.[94]

Additionally, on the homepage of each businesses' website, a clear and conspicuous link tilted "Do Not Sell My Personal Information" must be present, and a consumer must be able to click on the link without being required to create an account.[95] Although a business is prohibited from discriminating against consumers for exercising their opt-out rights, it may offer consumers certain financial incentives for allowing the sale of their personal information.[96]

3. Filing an action under the CCPA.

Under the CCPA, a consumer may file a civil action against a business that violates its duty to secure and protect the consumer's personal information from unauthorized disclosure, access, or theft.[97] The consumer may bring the action to recover: the greater of actual damages or an amount between $100 and $750 per consumer for each incident, an injunction,

---

[89] *Id.*
[90] *Id.*
[91] *Id.* § 1798.140(c)(1) (A)–(C).
[92] *Id.* § 1798.130(a)(1).
[93] *Id.* § 1798.130(a)(2).
[94] *Id.*
[95] *Id.* § 1798.135(a)(1).
[96] *See id.* § 1798.125(a)–(b).
[97] *Id.* § 1798.150(a)(1).

declaratory relief, or any other remedy the court sees fit.[98] Furthermore, if an entity intentionally violates the CCPA, it may be subject to a fine of up to $7,500 per each violation.[99]

Unless the consumer files suit for actual damages, the consumer must provide the business a thirty-day written notice, before bringing the action, that identifies the provisions of the CCPA that have been violated.[100] Further, there is no cause of action if the business cures the violation within the thirty days, provides a written statement to the consumer explaining the correction, and assures that the violation will not occur again.[101] If the business continues to violate the provision, after providing the written statement, the consumer may bring an action for breach of the written statement and for violating the provision.[102]

Once a consumer files an action, he or she must notify the Attorney General within thirty days.[103] Upon receiving the notice, the Attorney General has thirty days to notify the consumer that the Attorney General intends to prosecute the business for the violation, or that the consumer may not proceed with the action.[104] If the Attorney General does not prosecute the business within six months of notifying the consumer of his or her intent to do so, or takes no action within thirty days of receiving the consumer's notice, then the consumer may proceed with the action.[105]

Finally, the CCPA created a fund titled "Consumer Privacy Fund."[106] Twenty percent of all civil penalties paid for a violation, or the proceeds of a settlement action, are deposited to the fund to offset costs incurred by the state government in connection with the CCPA.[107] The remaining eighty percent is allocated to the jurisdiction in which the action was brought.[108]

C. The need for data privacy laws has been recognized by the European Union and the individual States.

While the CCPA represents the beginning of comprehensive data privacy law in the United States, the European Union ("EU") was the first to enact legislation regarding the rights and protection of consumers' personal

---

[98] *Id.* § 1798.150(a)(1)(A)–(B).
[99] *Id.* § 1798.155(b).
[100] *Id.* § 1798.150(b)(1). A consumer is not required to provide a written notice to the business if the consumer is "initiating an action solely for actual pecuniary damages suffered as a result of the alleged violations." *Id.*
[101] *Id.*
[102] *Id.*
[103] *Id.* § 1798.150(b)(2).
[104] *Id.* § 1798.150(b)(3)(A), (C).
[105] *Id.* § 1798.150(b)(3)(A).
[106] *Id.* § 1798.155(c)(1).
[107] *Id.*
[108] *Id.* § 1798.155(c)(2).

information.[109] However, as technology continues to grow, and with it the volume of available consumer data, several states have rapidly begun to recognize the need for regulation.[110]

1. The European Union is the first to enact a comprehensive data privacy regulation, affording consumers rights and protections regarding their personal information.

The General Data Protection Regulation ("GDPR") is the EU's data privacy law, which became enforceable on May 25, 2018.[111] Prior to the GDPR, data privacy in the EU was protected under an outdated law, the Data Protection Directive 95/46/EC, which was enacted in 1995, a time before social media and the cloud, when only one percent of European citizens used the internet.[112] Due to modern technology, with smart phones and companies like Google and Facebook collecting massive amounts of personal information, the EU determined that it was time to upgrade its data privacy laws to better protect its citizens.[113] The GDPR affects all businesses, regardless of their location, that offer goods or services to citizens within the EU.[114] Additionally, the regulation applies to any entity that collects, records, stores, retrieves, discloses, or uses personal data as part of a filing system.[115]

Under the GDPR, personal data is defined as any information that can be used to directly or indirectly identify a person.[116] Entities governed by the GDPR may collect personal data so long as collection is transparent.[117] However, in selective situations affirmative consent must be given by the consumer before collection can occur, and companies are responsible for proving that consent has been obtained.[118] Consumer data can only be collected for specific and legitimate purposes, and the information collected must be relevant and necessary to achieve the claimed purpose.[119] Further,

---

[109] *See generally How Did We Get Here? An Overview of Important Regulatory Events Leading Up to the GDPR*, EU GDPR PORTAL, https://eugdpr.org/the-process/how-did-we-get-here/ (last visited Jan. 15, 2020).

[110] *See generally* Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, DATA PROT. REPORT (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

[111] *See generally How Did We Get Here? An Overview of Important Regulatory Events Leading Up to the GDPR*, *supra* note 109.

[112] *Id.*

[113] Wall Street Journal, *GDPR: What Is It and How Might It Affect You?*, YOUTUBE (May 21, 2018), https://www.youtube.com/watch?v=j6wwBqfSk-o.

[114] Nicholas R. Merker & Deepali Doddi, *The GDPR Compliance Deadline Is Looming – Are You Prepared?*, PRATT'S PRIVACY AND CYBERSECURITY L. REP. (May 1, 2018), https://www.icemiller.com/MediaLibraries/icemiller.com/IceMiller/PDFs/publications/GDPR-Pratt-s-Privacy-Cybersecurity.pdf.

[115] *See* GDPR, 2016 O.J. (L 119) 2, https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04. The regulation does not affect a natural person who collects, records, stores, retrieves, discloses, or uses personal data as part of a filing system for purely personal or household activities. *Id.* at 2.

[116] *Id.* at 3.

[117] *Id.* at 6.

[118] *Id.* at 7, 9.

[119] *Id.* at 7.

companies that have collected personal data are accountable for securing and protecting the information from unlawful disclosure, theft, or use, and must implement data-protection principles, which are reviewed for compliance by the Member State's supervisory authorities.[120]

When personal data is collected, the entity must communicate with the citizen: what information has been collected and why; the length of time for which the information will be stored; his or her right to have the collected information erased; and the identity and contact information of any recipient or third party who will also receive the personal data.[121] Furthermore, a citizen may also obtain such information from a company at any time, and the company must provide the information free of charge.[122]

At any time, a citizen may request that the personal information collected about him or her be erased, and the entity must erase said information without undue delay.[123] Under the GDPR, citizens may also control how their data is used in certain circumstances, by restricting the purposes for which their information is processed.[124]

Organizations with more than 250 employees are responsible for maintaining an extensive and easily accessible record of all activities pertaining to the collection and use of personal information.[125] In the event of a breach of personal information, an entity must notify affected citizens within seventy-two hours.[126] Further, the entity must communicate the nature of the breach by describing the categories of data and the number of records concerned, the information obtained, the consequences of the breach, and the actions taken to combat the adverse effects of the breach.[127] Organizations that monitor data on a large scale must employ a Data Protection Officer ("DPO"), who is responsible for proper and timely handling and resolution of all personal data issues.[128] The DPO's contact information must be easily available to citizens.[129] For lesser offenses, noncompliance or infringements under the GDPR can result in a fine in the greater amount of ten million euro or two percent of the company's total worldwide annual turnover of the

---

[120] *Id.* at 7, 22. "'[S]upervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51" of the GDPR. *Id.* at 5. Article 51 requires each Member State to "provide for one or more independent public authorities to be responsible for monitoring the application of" the GDPR. *Id.* at 48.

[121] *Id.* at 13–14.

[122] *Id.* at 16–17.

[123] *Id.* at 17.

[124] *Id.* at 18. Processing is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, [organization], structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." *Id.* at 3.

[125] *See generally id.* at 27–28.

[126] *Id.* at 29.

[127] *Id.*

[128] *Id.* at 33.

[129] *See id.* at 12–13.

preceding financial year.[130] Fines for severe offenses may be imposed up to the greater of twenty million euro or four percent of the company's total worldwide annual turnover of the preceding financial year.[131]

2. State legislation regarding consumer data protection.

While the CCPA is currently the only enacted comprehensive data privacy law in the United States, which offers consumers protection, transparency, and control over personal information most akin to the GDPR, state legislation regarding data privacy has recently transpired throughout the United States.[132] As of March 2018, breach notification laws have been enacted in all fifty states.[133] In the event of a data breach, these laws require businesses to notify all affected consumers.[134] California and the EU have set the trend for legislation concerning a consumer's right to control their personal data and protection against misuse of information. Currently, two states have already introduced their own version of a comprehensive data privacy statute, comparable to that of either the CCPA or GDPR.[135] Additionally, several states have followed suit by enacting laws requiring businesses to safeguard consumers' personal information, beyond mere data breach notification.[136]

a. Washington introduces comprehensive data privacy legislation akin to the CCPA.

On January 18, 2019, the Washington Privacy Act ("WPA") was introduced in the State's Senate.[137] The WPA would affect businesses, regardless of their location, that either: (1) process or control the personal data of at least 100,000 Washington consumers, or (2) obtain more than fifty percent of their revenue from selling personal information, and process the data of at least 25,000 Washington consumers.[138] Under the WPA, each business must appoint a controller and a processor.[139] The controller must be a "natural or legal person which, alone or jointly with others, determines the

---

[130] *See id.* at 70–72.

[131] *See id.*

[132] *See generally* Serrato et al., *supra* note 110.

[133] *Id.*

[134] *Id.*

[135] *See generally* S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019); H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019).

[136] Serrato et al., *supra* note 110.

[137] *Comparing the Washington Privacy Act (WPA) to the California Consumer Privacy Act (CCPA)*, KLEIN MOYNIHAN TURCO (Feb. 15, 2019), http://www.kleinmoynihan.com/comparing-the-washington-privacy-act-wpa-to-the-california-consumer-privacy-act-ccpa/.

[138] S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019). Process is defined as "any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion, or destruction." *Id.* § 3(11).

[139] *See id.* § 5.

purposes and means of the processing of personal data."[140] A processor is a person who "processes personal data on behalf of the controller."[141]

The WPA affords consumers the right to request information regarding the personal data a business processes about them, and whether any of his or her personal data has been sold to third parties.[142] Upon receiving the request, the controller must provide the consumer with the requested information within thirty days, free of charge.[143] Additionally, a consumer may request that the controller correct any inaccurate or incomplete personal data, and the controller must correct the information without undue delay.[144]

A controller must comply with a consumer's request to delete his or her personal data if: the information is no longer needed relative to the purpose for which it was collected; there is no legitimate reason for why the business is processing the information; the information is used directly for marketing purposes; or the personal data was unlawfully processed.[145] Further, if the controller is obligated to delete the consumer's personal data, he or she must take reasonable steps to inform any third parties who have also obtained the information.[146]

Under the WPA, businesses must comply with transparency requirements.[147] These provisions direct businesses to provide consumers with a clear and meaningful privacy notice, which communicates: "[t]he categories of personal data collected"; the purpose of collecting each category; how the information is used and whether it is disclosed to any third parties; the rights of the consumer; and whether the information is used for profiling purposes.[148] Moreover, if the collected data is used for profiling purposes, the business must "includ[e] meaningful information about the logic involved and the significance and envisaged consequences of the profiling."[149]

The Attorney General is responsible for bringing an action to enforce the WPA.[150] If a controller violates a provision under the WPA, he or she is given thirty days to cure the violation.[151] If the violation is not cured, the controller "is subject to an injunction and liable for a civil penalty not more

---

[140] *Id.* § 3(4).
[141] *Id.* § 3(12).
[142] *Id.* § 6(1).
[143] *Id.* § 6(9)(b).
[144] *Id.* § 6(2)
[145] *Id.* § 6(3)(a)(i)–(iv).
[146] *Id.* § 6(3)(b).
[147] *See id.* § 7.
[148] *Id.* § 7(1)(a)–(d), (2).
[149] *Id.*
[150] *Id.* § 12(2).
[151] *Id.*

than [$2,500] for each violation or [$7,500] for each intentional violation."[152]

b. Texas introduces a comprehensive data privacy law.

On March 8, 2019, Texas introduced the Texas Privacy Protection Act ("TPPA").[153] Obligations of the TPPA apply to entities that do business in the state, have over fifty employees, collect personal identifying data of over 5,000 individuals, and either have an annual gross revenue greater than $25 million, or obtain at least fifty percent of its "annual revenue by processing personal identifying information.[154]

Under the TPPA, a business is prohibited from collecting personal identifying information, unless the collection thereof "is relevant and necessary to accomplish the purpose for which the information was collected," and the purpose is specifically communicated to the consumer.[155] Further, a business is prohibited from processing personal identifying information unless: the consumer affirmatively consents; the information is pertinent to achieving the purpose of processing the data; the purpose is explicitly communicated to the consumer; and "the information is processed only to the extent necessary to achieve one or more of those purposes."[156]

Businesses are required to implement a documented data security program to establish safeguards regarding personal identifying information.[157] Further, under the TPPA, businesses must provide a notice to consumers before collecting personal data, written in plain and clear language, and displayed in a conspicuous location at the business and on its website.[158] The notice must contain the categories of information processed, the purpose of processing such information, and whether the information is shared with any third parties.[159] Finally, businesses are compelled to adopt a privacy policy, publicly available to consumers, which articulates and describes whether the business uses the personal data to make predictions or provide analysis, and includes an easy method for consumers to gain access to the information collected about them.[160]

Under the TPPA, businesses must implement an accountability program to set procedures to respond to violations and data breaches, and they

---

[152] *Id.*

[153] H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019).

[154] *Id.* § 541.003.

[155] *Id.* § 541.051.

[156] *Id.* § 541.052. "'Processing' means any operation or set of operations that are performed on personal identifying information or on sets of personal identifying information, including the collection, creation, generation, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, or dissemination of the information or otherwise making the information available." *Id.* § 541.002(6).

[157] *Id.* § 541.053.

[158] *Id.* § 541.054.

[159] *Id.*

[160] *Id.* § 541.055.

must develop internal enforcement and discipline procedures for non-compliance.[161] Finally, the Attorney General may bring an action against a business to recover a civil penalty of up to $10,000 per violation.[162]

c. Vermont enacts legislation to protect consumers against the data broker industry.

On May 22, 2018, the State of Vermont enacted House Bill 764 ("HB 764"), for the purpose of providing consumers protection against the data broker industry.[163] Under HB 764, data brokers are defined as any business that collects and sells the personal information of Vermont consumers, with whom the business does not have a direct relationship.[164] Although HB 764 does not offer consumers protection against businesses they have a direct relationship with, Vermont determined that because the data broker industry is typically unknown to consumers, greater transparency and regulation is necessary.[165]

HB 764 requires data brokers to register with the state annually, pay a $100 registration fee, and disclose information to the state regarding the business's data collection practices, purchaser credentialing activities, opt-out procedures, and security breaches.[166] Additionally, data brokers must implement an information security program that meets the minimum safeguard features described in HB 764.[167]

Finally, HB 764 provides consumers with even greater protections against credit reporting agencies. Upon a consumer's request, credit reporting agencies must disclose all the information collected about the consumer, along with the names of users who have requested information regarding the consumer within the last twelve months.[168] The information must be conveyed to the consumer in a clear and concise way.[169]

d. Colorado legislation requires covered businesses to protect personal identifying data.

Colorado enacted House Bill 1128 ("HB 1128") on May 29, 2018, to provide its citizens with stronger consumer data privacy protection.[170] While HB 1128 predominantly compels covered businesses to follow specific notification requirements in the event of a data breach, it also affords

---

[161] *Id.* § 541.058.
[162] *Id.* § 541.101.
[163] H.B. 764, Gen. Assemb., 74th Biennial Sess. (Vt. 2017).
[164] *Id.* § 1(b)(1)(A)(I).
[165] *Id.* § 1(a)(1)(E)(ii).
[166] *Id.* § 2446(a).
[167] *Id.* § 2447(a)(1).
[168] *Id.* § 2480b(a)(1).
[169] *Id.*
[170] H.B. 1128, 71st Gen. Assemb., 2d Reg. Sess. (Co. 2018).

Colorado consumers with protections regarding personal identifying data.[171]

Under HB 1128, businesses that retain consumers' personal identifying information must develop a written policy regarding the destruction of the data.[172] Covered businesses must destroy data containing personal information when said data is no longer needed.[173] In addition, businesses are required to adopt and maintain security procedures and safeguards to protect consumers' personal identifying information from unlawful use, access, or disclosure.[174] Finally, under HB 1128, businesses that disclose personal identifying information to third parties must ensure those third parties also implement and uphold security procedures and safeguards to protect consumer data.[175]

3. Proposed federal legislation concerning consumer data privacy and protection.

While California is currently the only state to have enacted a comprehensive consumer data privacy law, as explained above, a "patchwork of state data privacy regimes" have started to develop.[176] Although currently no federal law has been passed—and several proposed bills concerning the issue have failed—members of Congress continue to draft bills regarding consumer data privacy rights and protection.[177]

In November of 2018, Senator Ron Wyden of Oregon released a discussion draft of legislation titled the Consumer Data Protection Act of 2018 ("CDPA").[178] This comprehensive data privacy legislation, like the GDPR or CCPA, requires businesses to provide greater transparency of data collection and use, and provides consumers with affirmative data privacy

---

[171] *See generally id.*

[172] *Id.* § 1(1). Personal identifying information is "a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data, . . . an employer, student, or military identification number; or a financial transaction device." *Id.* § 1(2)(b).

[173] *Id.* § 1(1).

[174] *Id.* § 2(1).

[175] *Id.* § 2(2).

[176] Joseph P. Facciponti & Maxwell Thompson, *Will New Congress Pass A National Data Protection Law?*, LAW360 (Jan. 4, 2019), https://www.law360.com/articles/1115448.

[177] The Customer Online Notification for Stopping Edge-provider Network Transgressions Act ("CONSENT Act") was introduced in the Senate on April 10, 2018. S. 2639, 115th Cong., 2d Sess. (as introduced in the Senate, April 10, 2018). This failed bill would have required the FTC to develop and establish privacy policies for entities that provide services to consumers over the internet ("edge providers") and require consumers to opt-in by affirmatively consenting to edge provider's use of his or her data. *Id.* The Information Transparency & Personal Data Control Act was introduced in the House on September 24, 2018. H.R. 6864, 115th Cong. 2d Sess. (as introduced in the House, Sept. 24, 2018). This failed bill would have required covered businesses to receive affirmative consent from consumers before collecting, sharing, storing, or selling consumer data, and afforded the FTC the power to regulate. *Id.* Additionally, entities would have to adopt privacy and data use policies and communicate said policy with consumers in clear and easy to understand language. *Id.*

[178] RON WYDEN, THE CONSUMER DATA PROTECTION ACT OF 2018 DISCUSSION DRAFT, https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20one%20pager%20Nov%201.pdf (last visited Jan. 15, 2020).

rights.[179]

The proposed legislation would be enforced and regulated by the FTC, and would create a system titled "Do Not Track," which would let consumers opt-out of data sharing, thus preventing covered businesses from sharing the consumer's personal information with third parties.[180] Businesses obligated by the CDPA are entities that have had "greater than $50,000,000 in average annual gross receipts for the [three]-taxable-year period preceding the [most recent] fiscal year," and that collect the personal information of more than 1,000,000 consumers annually.[181] While covered businesses cannot require consumers to remain opted-in, the business is allowed to charge opted-out consumers a fee to use its products or services.[182] However, the fee cannot be greater than the average amount the business would have gained had the consumer remained opted-in.[183]

Additionally, upon a written request from a consumer, a covered business must provide the consumer, free of charge and within thirty business days, the personal information collected about the consumer and the identity of any third party with whom the personal information was shared.[184] A consumer may challenge any information he or she deems inaccurate, and the business must investigate the challenged information and correct any inaccuracies.[185] Civil penalties may be sanctioned in the greater amount of $50,000 per violation or four percent of the company's annual revenue.[186]

Under the discussion draft, covered businesses must submit an annual data protection report confirming whether the business complied with the regulation.[187] If the business did not fully comply, it must describe in the report "which regulations were violated and the number of consumers whose personal information was impacted."[188] Additionally, criminal penalties may be sanctioned up to $5,000,000 and twenty years imprisonment if a business intentionally and falsely states that it complied with the regulation.[189]

III. ANALYSIS

A comprehensive data privacy regulation is needed in the United

[179] Chris Liedle, *Oregon Lawmaker Wants to Limit Companies' Use, Sharing & Selling of Your Personal Data*, KATU (Jan. 8, 2019), https://katu.com/news/local/oregon-lawmaker-plans-to-limit-companies-use-sharing-selling-of-your-personal-data.

[180] Consumer Data Protection Act, SIL18B29, 115th Cong. § 6(a)(1) (2d Sess. 2018), https://www.wyden.senate.gov/imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20Nov%201.pdf (last visited Jan. 15, 2020).

[181] *Id.* § 2(5)(B).

[182] *Id.* § 6(b)(1)(A)–(B).

[183] *Id.* § 6(b)(2).

[184] *Id.* § 7(b)(1)(D).

[185] *Id.* § 7(b)(1)(F).

[186] *Id.* § 4(1)(A).

[187] *Id.* § 5(a)(1).

[188] *Id.*

[189] *Id.* § 5(b)(1).

States, because as technology continues to grow, so does the amount of consumer data available and the possibility of consumer harm.[190] The collection, use, and sale of personal data represents a multi-billion-dollar infrastructure.[191] Unlike the reactive nature of the SEC, created to regulate the multi-trillion-dollar stock market industry in response to the devastation suffered by the market crash of 1929, Congress must enact regulation of data collection and use before serious exploitation and harm to consumers occur.[192] Despite the data privacy laws previously discussed, many consumers currently have no way of knowing what information has been collected about them, who has access to their information, how to fix incorrect data, and how to stop businesses from collecting their data.[193] The lack of transparency in data collection, use, and sales must be rectified to protect consumers from harm and to keep businesses accountable.

Although individual states recognize the need for data privacy regulations and have begun implementing such laws, a federal data privacy law is necessary to supersede state laws.[194] First, the CCPA is flawed and will have far reaching effects on businesses throughout the United States. Second, if states are left to enact their own comprehensive laws, similar to the CCPA, it will be too cumbersome for smaller businesses to adhere to all individual state laws; thus, inhibiting growth and innovation. If the positive aspects of the CDPA, CCPA, and GDPR are combined, a successful comprehensive data privacy regulation can be implemented in the United States to give consumers control of their private information; shed transparency on data collection, use, sales; and hold businesses accountable while still allowing innovation and growth to thrive.

A. Flaws in the CCPA.

1. The CCPA's anti-discrimination provision will create confusion.

While the CCPA has many positive aspects, the anti-discrimination provision is unclear and will create confusion.[195] This provision states, in relevant part:

> (1) A business *shall not discriminate* against a consumer because the consumer exercised any of the consumer's rights under this title, including but not limited to, by:

---

[190] *See, e.g.*, Kelly Sheridan, *Exposed Consumer Data Skyrocketed 126% in 2018*, DARKREADING (Jan. 15, 2020), https://www.darkreading.com/attacks-breaches/exposed-consumer-data-skyrocketed-126--in-2018/d/d-id/1333790.

[191] *The World's Most Valuable Resource is No Longer Oil, but Data*, *supra* note 1.

[192] U.S. SEC. AND EXCH. COMM'N, *supra* note 25.

[193] *See generally supra* Section II.

[194] *See generally supra* Section II.

[195] Assemb. B. 375, 2017-18 Reg. Sess. § 1798.25 (Cal. 2018) (enacted).

(A) Denying goods or services to the consumer.

(B) *Charging different prices or rates* for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

(2) *Nothing in this subdivision prohibits a business from charging a consumer a different price or rate*, or from providing a different level or quality of goods or services to the consumer, if that difference is *reasonably related to the value* provided to the consumer by the consumer's data.[196]

This provision effectively states that companies cannot discriminate against consumers who opt-out of collection, use, and sale of personal data, yet companies are permitted to incentivize consumers to remain opted-in.[197] The provision does not make clear the distinction between discrimination and incentive. Under the CCPA, discrimination exists when a company charges an opted-out consumer a different rate then a consumer who is opted-in; yet, the company may charge an opted-in consumer a lower rate than an opted-out consumer as an incentive.[198] The only distinction between these is that the lower rate offered to the opted-in consumer must be reasonable in relation to the value of the consumer's data.[199]

The difference between what constitutes discrimination verses an incentive is confusing at best, and at first glance it appears the section states two contradictory provisions back-to-back.[200] To make matters worse, the CCPA is silent on what constitutes, or how to determine, the reasonable value of a consumer's data.[201] Thus, a company has no guideline to determine the incentivized lower price to the opted-in consumer (or effectively a higher price to the opted-out consumer, which under the provision is discrimination—confusing, right?). Because there is seemingly only a slight difference between discrimination and incentive, this can cause harm to businesses that attempt, but fail to comply. Moreover, as the CCPA applies

[196] *Id.* (emphasis added).
[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *See generally id.*
[201] Assemb. B. 375, 2017-18 Reg. Sess. (Cal. 2018) (enacted).

to businesses regardless of their location, a smaller business across the country may have increased difficulties in compliance, because it will be harder to contact the proper authority in California with questions or seeking guidance regarding confusing provisions.[202]

The flawed construction of the anti-discrimination provision highlights one reason why a federal data privacy law should be enacted to supersede state laws. While the CCPA has many positive aspects, because its reach affects businesses regardless of their location, flaws such as this can create heavy burdens and potentially high penalties on smaller businesses outside of California, who do not have representation in the California state government to seek amendments.

2. The CCPA's enforcement provisions impose unworkable obligations upon the Attorney General and will hinder its effective execution.

The CCPA has thrust "unworkable obligations" upon the Attorney General, which will impede "vigorous oversight and effective enforcement" of the protections afforded to consumers.[203] Unless a consumer brings suit against a business for actual damages, the Attorney General has absolute control on whether the consumer is allowed to go forth with litigation.[204] If a consumer wants to bring suit against a business that has violated a provision under the CCPA, he or she must notify the Attorney General within thirty days of filing the action.[205] After receiving notice, the Attorney General has the power to prohibit the consumer from bringing suit in two ways: (1) the Attorney General may expressly inform the consumer that he or she cannot proceed with the case, or (2) the Attorney General may elect to personally prosecute the business—thereby preventing the consumer from bringing suit.[206]

This provision is problematic for three reasons. First, the provision vests the Attorney General with the authority to determine whether a consumer may bring suit.[207] Thus, the Attorney General must take on an additional role as a filter for consumers' civil claims against businesses. This role is problematic because it affords the Attorney General the judicial power of judging each claim on the merits.

Second, the CCPA does not provide any parameter for why or when

---

[202] *See infra* Section III.A.2.

[203] Letter from Xavier Becerra, Cal. Attorney Gen., to Ed Chau, Assemblymember, Cal. State Assembly, and to Robert Herzberg, Senator, Cal. State Senate (Aug. 22, 2018), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical.

[204] Assemb. B. 375, 2017-18 Reg. Sess. § 1798.150(b) (Cal. 2018) (enacted).

[205] *Id.* § 1798.150(b)(2).

[206] *Id.* § 1798.150(b)(3).

[207] Letter from Xavier Becerra, *supra* note 203.

the Attorney General can or should prohibit a consumer from bringing suit.[208] Lack of guidance also hurts consumers. Consumers with valid claims may be unwilling to bring action, for fear of wasting time and money initiating a suit that may be struck down by the Attorney General. Conversely, consumers with invalid claims may waste time and money in commencing an action that is ultimately barred by the Attorney General. If the provision explained reasons or circumstances that would allow the Attorney General to prohibit action and described situations in which the Attorney General could not prohibit action, consumers could avoid wasting resources initiating a suit that did not meet the threshold or confidently initiate suit knowing their claims were actionable.

Finally, the provision thrusts excessively burdensome obligations upon the Attorney General.[209] The Attorney General has already expressed concern regarding the difficulties, and depleting resources, his office will sustain because of the duties imposed under the CCPA.[210] If the Attorney General's predictions are correct, and the magnitude of duties results in insufficient resources—thereby weakening means of enforcement—businesses may stop complying with the CCPA, knowing they are unlikely to be held accountable. Further, the Attorney General is required to provide unlimited legal counsel to businesses regarding their obligations under the CCPA.[211] These new duties will inevitably, and unnecessarily, exhaust the Attorney General's time and resources.

3. The provision that allows a business to avoid litigation by actually curing its violation is confusing and undefined.

Under the CCPA, unless bringing a lawsuit for actual damages, the consumer must alert the business of its alleged violation via a written notice.[212] After forewarning the business, the consumer must notify the Attorney General of his or her intent to initiate action.[213] The business is then provided with thirty days to cure the violation; if the business successfully cures, it must notify the consumer, and the consumer is barred from bringing suit.[214] Unfortunately, the CCPA does not provide a definition for "cure," nor does the provision explain which violations are even curable.[215] If a consumer wishes to initiate an action arising from a data breach, does the fact that the business has now increased security "cure" the violation, and thereby bar the consumer, whose information has already been compromised, from bringing

---

[208] *See generally* Assemb. B. 375, 2017-18 Reg. Sess. (Cal. 2018) (enacted).
[209] Letter from Xavier Becerra, *supra* note 203.
[210] *Id.*
[211] *Id.*
[212] Assemb. B. 375, 2017-18 Reg. Sess. § 1798.150(b)(1) (Cal. 2018) (enacted).
[213] *Id.*
[214] *Id.*
[215] *See generally* Assemb. B. 375, 2017-18 Reg. Sess. (Cal. 2018) (enacted).

suit?

Additionally, the CCPA provides no inspection of the business to determine whether the violation was in fact cured.[216] If the business sends the consumer a written notification informing the consumer that the violation has been cured, does the consumer have to take the business's word? If a consumer receives notice that the violation has been cured, but does not believe the business, or does not agree that the mitigating steps have cured the violation, the provision is silent on what the consumer should do.[217] Although the consumer may bring the original claim and pursue breach of the written statement if it is found to be false, this requires the consumer to be harmed yet again before initiating action and still does not describe how the consumer can even go about determining the statement's falsity.[218] Thus, it appears the consumer is helpless upon receiving a notification by the business that the violation has been cured.

B. A unified data privacy law will protect the Nation's businesses.

Currently, all fifty states have enacted data breach notification laws.[219] Thus, because businesses are expected to adequately comply with fifty data breach notification state laws, adherence to fifty comprehensive data privacy laws is conceivable as well.[220] However, breach notification is just one, fairly simple, requirement. While there may be slight differences between the states' laws, the heart of each regulation requires the business to notify consumers when their personal information has been illegally obtained.[221]

The CCPA is comprehensive and encompasses many different provisions, unlike mere data breach notification laws.[222] The sheer volume of requirements contained within comprehensive data privacy laws will make compliance with fifty different state laws exceedingly difficult and expensive.[223] Further, two states have already followed California and introduced their own comprehensive data bills.[224] Thus, the trend towards enactment of comprehensive data laws will not stop with the EU and California, and compliance with various state laws will become a reality.

While large companies will likely have sufficient resources, smaller

---

[216] *Id.*

[217] *Id.*

[218] *Id.* § 1798.150(b)(1).

[219] Serrato et al., *supra* note 110.

[220] *See generally* R. David Lane Jr., *Legal Obligations When a Data Breach Invokes the Laws of Multiple Jurisdictions*, N.Y. L.J. (July 12, 2019, 11:30 AM), https://www.law.com/newyorklawjournal/2019/07/12/legal-obligations-when-a-data-breach-invokes-the-laws-of-multiple-jurisdictions/.

[221] *Id.*

[222] *See generally* Assemb. B. 375, 2017-18 Reg. Sess. (Cal. 2018) (enacted).

[223] *See generally supra* Section II.

[224] *See generally* S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019); H.B. 4390, 86th Leg., Reg. Sess. (Tex. 2019).

businesses, those that have just met the minimum threshold to be obligated and have restrictive means compared to large companies, will face the biggest impact.[225] Smaller businesses will have to choose between allocating additional funds to ensure compliance with all fifty state laws, or risk litigation and large monetary penalties for violations. Compliance with fifty different laws will be cumbersome and exceedingly expensive, as opposed to one federal statute; thus, inhibiting growth and innovation, especially for smaller businesses or start-ups.

C. Proposed requirements for a federal data privacy law.

A successful comprehensive data privacy law should embody the core values of the CCPA: control, transparency, and accountability.[226] To best achieve a regulatory scheme that protects consumers and holds businesses accountable, without inhibiting growth and innovation, the federal law should adopt provisions akin to the positive aspects of the CCPA, CDPA, GDPR, and give regulative authority to the FTC.

1. Control

The "Do Not Track" system, proposed within the CDPA discussion draft, should be adopted in the federal data privacy statute. This system will give consumers sufficient control over their data by allowing them to easily opt-out of data sharing, thereby prohibiting a business from sharing their data with third parties.[227]

Although the GDPR requires some businesses to receive affirmative consent before consumers' data may be shared with third parties, the CDPA's "Do Not Track" system would create a reasonable balance between the interest of both consumers and businesses.[228] The goal of a federal data privacy law should be to give consumers choice and control over their personal information. While legislation will provide consumers with these rights, at the same time it will require businesses to embrace new obligations and duties. However, the magnitude of these new obligations and duties must not have the actual effect of impeding upon growth and innovation of businesses. Thus, so long as the "Do Not Track" system is placed conspicuously on businesses websites, allows consumers to easily opt-out,

---

[225] *See, e.g.*, U.S. CHAMBER OF COMMERCE FOUND., THE REGULATORY IMPACT ON SMALL BUSINESS: COMPLEX. CUMBERSOME. COSTLY. 4–6 (Mar. 2017), https://www.uschamberfoundation.org/smallbizregs/assets/files/Small_Business_Regulation_Study.pdf; *see also* Eric Goldman, *41 California Privacy Experts Urge Major Changes to the California Consumer Privacy Act*, TECHNOLOGY & MARKETING LAW BLOG, (Jan. 17, 2019), https://blog.ericgoldman.org/archives/2019/01/41-california-privacy-experts-urge-major-changes-to-the-california-consumer-privacy-act.htm.

[226] Int'l Ass'n of Privacy Prof'ls, *supra* note 53, at 4:21.

[227] Consumer Data Protection Act, SIL18B29, 115th Cong. § 7(d) (2d Sess. 2018); *id.* § 6(a)(1).

[228] 2016 O.J. (L 119) 6(1)(f); Consumer Data Protection Act, SIL18B29, 115th Cong. § 7(d) (2d Sess. 2018).

and is overseen by the FTC, the system will provide reasonable and sufficient control to consumers over their personal information.

Unlike the CCPA's confusing anti-discrimination provision, the CDPA is straightforward, and clearly allows businesses to charge opted-out consumers a higher fee to use its products or services.[229] While the CCPA's "reasonably related value" incentive provision is murky and undefined, the CDPA provides that a business may not charge an opted-out consumer a fee higher than the average dollar amount the business would have gained had the consumer remained opted-in.[230] Although the CDPA does not describe how the business must determine the average amount it would have gained, its provision is superior to the CCPA's because it at least provides guidance on how to establish an acceptable fee to remain in compliance.

2. Transparency

A federal regulation should provide consumers with greater transparency regarding data collection and use practices. It can be understood that most consumers want transparency in data collection and use practices for similar reasons of why consumers wanted restaurants to display the number of calories for each item on the menu.[231] For example, consumers were shocked when they watched the documentary *Super-Size Me*, and learned about how unhealthy and how many calories were in food items at McDonalds.[232] As shown in the documentary, at that time it was difficult for a consumer to obtain the nutritional information of menu items.[233] Now, when people go to McDonalds, or most commercial restaurants, the amount of calories are listed directly next to each food item.[234] That is not to say people stopped eating Big Macs due to McDonald's transparency of the calories it

---

[229] Assemb. B. 375, 2017-18 Reg. Sess. § 1798.25(a) (Cal. 2018) (enacted); SIL18B29, 115th Cong. 2d Sess. § 6(b)(1), (2).

[230] Assemb. B. 375, 2017-18 Reg. Sess. § 1798.25(b) (Cal. 2018); SIL18B29 § 6(b)(2).

[231] *See, e.g.*, *Pros and Cons of Calorie Counts on Menus: Should Your Restaurant Provide Nutritional Information*, MENUCALC (Oct. 16, 2017), https://www.menucalc.com/2017/10/16/pros-and-cons-of-calorie-counts-on-menus-should-your-restaurant-provide-nutritional-information/; Jennifer Frighetto, *Fifty Nine Percent of Consumers Around the World Indicate Difficulty Understanding Nutritional Labels*, NIELSEN (Jan. 25, 2012), https://www.nielsen.com/ca/en/press-releases/2012/fifty-nine-percent-of-consumers-around-the-world-indicate-diffic/.

[232] *See generally* Meghan Demaria, *How Super Size Me Really Changed Our Diets*, REFINERY29 CIVIL EATS (Jan. 3, 2017, 1:30 PM), https://www.refinery29.com/en-us/2017/01/124346/fast-food-industry-changes-nutrition-facts. *Super Size Me* is a documentary created by Morgan Spurlock, who ate nothing but McDonald's for 30 days. Further, every time Spurlock was asked if he wanted to super size his meal, he said yes. Throughout the 30 days Spurlock consumed around 5,000 calories per day and gained 24 pounds. *Super Size Me*, WIKIPEDIA, https://en.wikipedia.org/wiki/Super_Size_Me, (last visited Jan. 15, 2020); *Id.*

[233] Paula Crossfield, *After 'Super Size Me': In Conversation with Morgan Spurlock*, CIVIL EATS (Nov. 16, 2010), https://civileats.com/2010/11/16/after-super-size-me-in-conversation-with-morgan-spurlock/.

[234] *Menu Labeling Requirements*, U.S. FOOD & DRUG ADMINISTRATION, https://www.fda.gov/Food/GuidanceRegulation/GuidanceDocumentsRegulatoryInformation/LabelingNutrition/ucm515020.htm (last visited Jan. 15, 2020).

contains.[235] Rather, consumers appreciate the transparency because it allows them to be generally informed when choosing their meal. Thus, like calories on a menu, consumers want transparency in data collection and use not only to protect them from harm, but also to be generally informed about what is being collected about them and why.[236]

The comprehensive federal data privacy regulation should provide consumers with transparency rights akin to those found in the CCPA. Consumers should have the right to request that businesses disclose, free of charge, the categories of personal information collected about the consumer, the purpose of the category of information, and how the category of information is used.[237] This right can also help combat the use of insensitive category names, like those reported by the FTC, as businesses will be less inclined to create rude and offensive category names if they know consumers can observe them.[238]

Further, as described in the CCPA, to balance the burden of disclosure on businesses under the federal law, a business should only be required to disclose information to each individual consumer twice every twelve-months.[239] The law should compel businesses to easily allow consumers to request a disclosure, by inserting a "My Information" tab directly next to the "Do Not Track" system. In the event the consumer discovers the business has inaccurate information regarding the consumer, the business must be required to correct the information without undue delay. Finally, like under the CCPA, consumers should be given the right to demand that a business delete any, or all, of the information collected about them.[240]

3. Accountability

As proposed in the CDPA, the federal comprehensive data privacy law should be regulated by the FTC.[241] Businesses should be required to annually submit a written report to the FTC, confirming compliance with all provisions under the law, or describing any violations and data breaches the business experienced throughout the year. This written statement will keep businesses accountable and provide a basis for prosecution if it is found to contain false information. If a business is discovered to have unintentionally

---

[235] *See* Meghan de Maria, *17 Crazy Facts About the Big Mac You Never Knew*, EAT THIS, NOT THAT! (Jan. 16, 2019), https://www.eatthis.com/big-mac-facts/. In fact, Big Macs remain the second-most-popular item on McDonald's menu.

[236] Sudipto Ghosh, *SAP Survey: U.S. Consumers Want Better Service and More Transparency in Data Collection*, MKTG. TECH. INSIGHTS (Jan. 23, 2018, 4:27 PM), https://martechseries.com/analytics/b2b-data/us-consumers-want-better-service-and-more-transparency-in-data-collection/.

[237] *See generally* Assemb. B. 375, 2017-18 Reg. Sess., sec 3(a)–(d) (Cal. 2018) (enacted).

[238] FTC Press Release, *supra* note 3.

[239] Assemb. B. 375, 2017-18 Reg. Sess., § 3(d) (Cal. 2018) (enacted).

[240] *Id.* § 1798 (a), (c).

[241] Consumer Data Protection Act, SIL18B29, 115th Cong. § 7(d)(2) (2d Sess. 2018); *id.* § 1798.150(a)(1)(A)–(B).

or unknowingly submitted false information, the business should be subjected to a fine. However, businesses found to have intentionally falsified the written report should be exposed to criminal penalties, including a hefty fine and imprisonment of those responsible for the intentional inclusion of the false information.

Additionally, the federal law should hold businesses accountable for adopting a policy that imposes safeguards to prevent data breaches.[242] The FTC should be responsible for describing the minimum safeguard requirements for compliance, and annually adjusting the standards if needed. Further, businesses should be required to annually send an updated version of their safeguard policies to the FTC. The FTC will determine and inform the business whether the policy meets the minimum standards for compliance. Failure to craft and adopt a policy that adheres to the minimum requirements should subject the business to prosecution, at the discretion of the FTC.

Finally, the federal law should afford consumers a private right of action, by allowing consumers to initiate civil litigation against a business for violations. Installing a private right of action is superior to the CCPA's provision, which requires the Attorney General to determine whether suit may be brought, because it reduces the obligation of funding the Attorney General, with taxpayer dollars, to act as a judge on the merits of civil cases.[243] However, like the CCPA, the federal statute should impose either (1) the greater of actual damages, or an amount between $100 and $750 per consumer for each incident; (2) an injunction; or (3) declaratory relief.[244] The relatively low damage award per violation will balance the private right of action from creating excessive or frivolous litigation, as consumers will be unlikely to endure court and attorney costs associated with bringing suit unless substantial violations have occurred.

IV. CONCLUSION

A comprehensive federal data privacy law that supersedes state law should be enacted to best balance consumer protection and business innovation. Media coverage regarding data breaches have made headlines and affected millions of consumers in the United States.[245] As the result of these breaches, not only have consumers experienced an invasion of their

---

[242] This requirement is similar to provisions found in the TPPA. *See supra* Section II.C.2.b.

[243] *See supra* Section III.A.2.

[244] *See* Consumer Data Protection Act, SIL18B29, 115th Cong. § 1798.150(a)(1)(A)–(B) (2d Sess. 2018).

[245] Davey Winder, *(Updated) 2 Billion Unencrypted Records Leaked in Marketing Data Breach – What to Do Next*, FORBES (Mar. 10, 2019), https://www.forbes.com/sites/daveywinder/2019/03/10/2-billion-unencrypted-records-leaked-in-marketing-data-breach-what-happened-and-what-to-do-next/#16b7aec6b0dc; Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html.

privacy, but also a loss of confidence and trust that businesses will protect their personal information.[246]

The GDPR and CCPA represent just the beginning of comprehensive data privacy regulation. Soon, businesses will be faced with compliance of a multitude of state laws.[247] Each of these laws contain a variation of requirements and penalties for violations.[248] It will be the responsibility of the business to adopt fifty different privacy and transparency policies to adhere to each state's respective law. This feat will be costly and will particularly inhibit smaller businesses who must allocate substantial resources to comply with each law, or face adjudication and penalties for violations.[249] Thus, enactment of a comprehensive federal law that supersedes state law will afford consumers with rights and protection over their personal information, while alleviating businesses from the costly hurdles of compliance with a multitude of state laws.

[246] *See* Nicholas King, *Customers Lose Confidence—Data Breaches Aren't Just About Fines*, IT GOVERNANCE (Jan. 29, 2019), https://www.itgovernanceusa.com/blog/customers-lose-confidence-data-breaches-arent-just-about-fines.

[247] *See supra* Sections II.A., II.C.2.

[248] *See supra* Sections II.A., II.C.2.

[249] *See supra* Section III.B.