THE iOS 14.5 UPDATE: A GAME CHANGER IN FEDERAL PRIVACY LAW

Chris Jones*

Cite as: Chris Jones, *The iOS 14.5 Update: A Game Changer in Federal Privacy Law*, 28 RICH. J.L. & TECH. 254 (2021).

* J.D., Gonzaga University School of Law. Acknowledgments and gratitude to Professor Drew Simshaw for his invaluable insights, feedback, and continuing support. Special thanks to the entire 2021-2022 editorial staff of the *Richmond Journal of Law & Technology* for their dedication, hard work, and flexibility.

ABSTRACT

From 1890, when the right to privacy was defined, to the 1973 debut of the Fair Information Practice Principles that set the "Gold Standard" for consumer privacy protection, to the FTC's request for a federal privacy law in 2000, the core expectations of privacy have remained the same. United States consumers have a right to privacy that requires notice and consent for the use of their personal information. The Apple iOS 14.5 update introduced App Tracking Transparency, providing consumers with the opportunity to affirmatively opt in or decline the tracking and sharing of their personal information. This update has shown that when faced with a simple, comprehensible choice to opt in to the sale of their personal information, only 15% of responding consumers in the United States consent to this invasive surveillance. The majority of online applications and websites currently track and share personal information without consumer knowledge or consent. Such data sharing subjects individuals to potential privacy harms, like discrimination, reputational damage, social stigmatization, and safety concerns. Absent a comprehensive federal privacy law, states have begun passing their own privacy laws creating a fragmented patchwork of regulation. This trend is leading away from pro-consumer fundamentals of privacy, increasingly favoring business backers. There have been calls for federal privacy legislation for decades. This article will be among the first to analyze the iOS 14.5 update and emerging state privacy laws. This article argues that United States consumers' thirst for privacy, as exemplified by the iOS 14.5 update results, should be utilized as an overarching guide for Congress when enacting comprehensive federal privacy law. By drawing from principles of the iOS 14.5 update and the European General Data Protection Regulation (GDPR), and from some features of recent state privacy laws, Congress should enact federal privacy legislation that applies to all businesses collecting consumer personal information and requires affirmative opt-in consent for data sharing and tracking. Consumers have spoken. It is time for Congress to utilize this data and provide a high level of privacy protection for all Americans.

I. INTRODUCTION

[1] Imagine that you place grocery orders online to pick up at your neighborhood store. While the retailer's website happens to have a Privacy Policy and Terms of Use at the bottom of its home page, you do not notice it as you enter your shopper's rewards card number and complete the transaction. Because you did not read the lengthy policies in the fine print, you are unaware that your personal data, including your phone number, home address, purchase history, and facial recognition scans taken while shopping at the store, will be sold to third-party data brokers and shared with other companies unless you complete an onerous process to opt out.[1] The data brokers then sell your personal information, including your purchases of sensitive medications and internet browsing history, to multiple advertising platforms, including social media companies. This information is compiled to create a personalized profile of your real-life habits and may be utilized to infer sensitive points like medical conditions or sexual orientation.[2] Imagine now that a friend you frequently spend time with happens to have a bladder condition for which they frequently purchase Depends undergarments. The tracking mechanisms embedded in the applications on your phones recognize you are in the same places at the same time; thus, they infer you may also have a bladder condition. It is no coincidence that after you visit your friend, you are bombarded with personalized ads for Depends when you log on to your social media platform. Your name and contact information have been included on lists of

[1] *See What Are Data Brokers—and What Is Your Data Worth?*, WEBFX (Mar. 16, 2020), https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ [https://perma.cc/AMR4-7FEF] [hereinafter *What Are Data Brokers*] (stating that data brokers comprise a "multi-billion dollar industry made up of companies who collect consumer data and sell it to other companies, usually for marketing purposes" and that many consumers are unaware this practice exists as data brokers do not collect data directly from consumers).

[2] *See generally* Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/ [https://perma.cc/E5UG-U5MN] (explaining how Target's algorithms utilized a teen girl's purchase history to correctly infer that she was pregnant).

consumers with bladder conditions that are openly sold by data brokers.[3] You are later denied employment because the business incorrectly inferred that you had a certain medical condition.

[2] Data brokers and advertisers have become the real consumers of the internet.[4] With help from Big Tech,[5] advertisers collect, trade, or sell every piece of a consumer's profile that can be derived from web browsing, online shopping, and internet searches.[6] With increased smartphone technology, advertisers track whether a consumer drove past a specific billboard advertisement before buying the advertised products.[7] Thousands of data points are for sale on virtually every American adult. Big Tech has become "increasingly precise" at predicting what you might do next, such as get a divorce or quit your job.[8] The biggest "repositories of intimate personal data" are maintained by Facebook and Google, who collect data on all consumers, whether or not they use the companies' products.[9] Over the past decade, Facebook and Google have created "an elaborate and invisible network of browsing bugs" that follow consumers around the internet,

[3] *See What Are Data* Brokers, *supra* note 1.

[4] *See* 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 [https://perma.cc/Q9U5-TKJ2].

[5] *See* Jessica Guynn, *Amazon, AT&T, Google push Congress to pass online privacy bill to preempt stronger California law*, USA TODAY (Sept. 26, 2018, 6:02 PM), https://eu.usatoday.com/story/tech/news/2018/09/26/amazon-att-google-apple-push-congress-pass-online-privacy-bill-preempt-stronger-california-law/1432738002/ [https://perma.cc/3M43-2B9J] ("Big Tech" refers to some of the largest United States-based technology and telecommunications companies. For example, Facebook, Google, Amazon, and Microsoft are considered part of Big Tech); *see also* Confessore, *supra* note 4.

[6] *See* Confessore, *supra* note 4.

[7] *See id.*

[8] *See id.*

[9] *See id.*

creating a "private surveillance apparatus of extraordinary reach and sophistication."[10]

[3] The core expectations of consumer privacy have remained the same since 1890.[11] American consumers have a right to privacy that requires notice and consent for the use of their personal information.[12] Consumers that "feel protected from misuse of their personal information feel free to engage in commerce."[13] While the Consumer Privacy Bill of Rights (CPBR)[14] had the right privacy concepts in 2012, Congress has failed to capitalize on opportunities by incessantly debating issues important to their financial backers, while drafting lengthy, complex proposals.[15] Such complexities only serve to line attorneys' pockets at the expense of consumer privacy. After the privacy principles of the CPBR were not converted into law, we have seen: interference with national elections;[16] Facebook's Cambridge Analytica scandal, where up to 87 million

[10] *See id.*

[11] *See History of Privacy Timeline*, INFO. & TECH. SERVS. U. MICH., https://safecomputing.umich.edu/privacy/history-of-privacy-timeline [https://perma.cc/L79B-ZQTK].

[12] *See* discussion *infra* Section III.

[13] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012) [hereinafter WHITE HOUSE PRIVACY REPORT].

[14] *See* discussion *infra* Section III.

[15] *See* Loree Bykerk & Ardith Maney, *Consumer Protection Policy Issues on the Congressional Agenda*, 125 POL. SCI. Q. 639, 640 (2010–11).

[16] *See* Confessore, *supra* note 4.

consumers had their personal information shared for political motives;[17] and unregulated data brokers that buy and sell our personality profiles as a commodity on the open market.[18]

[4] In 2020, there were 4,000 data broker companies worldwide.[19] "Acxiom, one of the largest [data brokering companies], has 23,000 servers collecting & analyzing consumer data, Data for 500 million consumers worldwide, and up to 3,000 data points per person."[20] Well over a thousand leading brands with store loyalty cards sell their customers' information, while eighty percent of United States email addresses are on file with a data broker.[21] Over 240 million consumers self-reported information through warranty registrations, contests, and marketing surveys that ended up in the hands of data brokers.[22] Data brokering has become a $200 billion dollar industry made up of brokers that sell lists of consumer contact information, including specific lists of individuals that fall into certain categories inferred

[17] John Hendel, *'Embarrassing': Congress stumbles in push for consumer privacy bill*, POLITICO: TECH. (July 12, 2019, 8:05 PM), https://www.politico.com/story/2019/07/12/congress-consumer-privacy-bill-1582540 [https://perma.cc/QFV7-UGZH].

[18] *See What Are Data Brokers*, *supra* note 1; *see also* Sharon R. Klein & Alex C. Nisenbaum, *California Legislature Passes Nation's Second 'Data Broker Registration' Law*, TROUTMAN PEPPER (Oct. 3, 2020), https://www.troutman.com/insights/california-legislature-passes-nations-second-data-broker-registration-law.html [https://perma.cc/3PL6-JH6M] (describing the regulation of data brokers is just beginning and how following Vermont's lead, California created a data broker registry in 2020, requiring data brokers to register with the California Attorney General).

[19] *What Are Data Brokers*, *supra* note 1.

[20] *Id.*

[21] *Id.*

[22] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 14 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/Q586-323E] [hereinafter FTC DATA BROKER REPORT].

by their activities.[23] For example, one company sold lists of 1,000 people with health conditions like depression, anorexia, and substance abuse.[24] Additionally, Facebook created partnerships with data brokers to merge their users' data, "linking real-world activities to those on the Web."[25]

[5] The harms of consumer privacy issues encompass a wide range of scenarios from discrimination, to economic loss, to emotional impairment.[26] The disclosure of personal data may affect a consumer's ability to obtain insurance, housing, employment, financial products, or admission to a nursing home; it may cause social stigmatization based on disease, mental health conditions, addictions, race, sexual preferences, political opinions, or religion; it may subject consumers to unfair business practices and unwanted fraudulent offers; and it may subject consumers to potentially dangerous situations due to the revelation of secret locations for domestic abuse victims or persons in witness protection programs, bullying, stalking, ransomware, or blackmail.[27]

[6] Privacy policies are not enough to protect consumers from privacy harms. Privacy policies generally exist to explain what the platform does with the user's information, including with whom such information is

[23] *See What Are Data Brokers*, *supra* note 1 (stating that data brokers "aggregate[d] and model[ed] the purchase history of 190 million individuals from more than 2600 merchants"); FTC DATA BROKER REPORT, *supra* note 22, at 14.

[24] *What Are Data* Brokers, *supra* note 1.

[25] Patrick Turner, *Has Big Data Made Anonymity Impossible?*, MIT TECH. REV. (May 7, 2013), https://www.technologyreview.com/2013/05/07/178542/has-big-data-made-anonymity-impossible/ [https://perma.cc/4TGX-345J].

[26] *See* Lothar Determann, *Healthy Data Protection*, 26 MICH. TELECOMM. & TECH. L. REV. 229, 256 (2020).

[27] *See id*.; *see also* Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 465–66 (2018).

shared.[28] Typically filled with technical terms and legal language, they are read by consumers attempting to protect their personal information.[29] Many privacy policies are difficult for consumers to understand and do not accord with the transparency principle meant to provide consumers with an easily understandable format.[30]

[7] "As of January 2021, there were approximately 269.5 million mobile internet users in the United States, representing over 90 percent of all active internet users nationwide. Meanwhile it was found that among the 240 million individuals that used social media, over 233 million accessed their accounts via mobile."[31] The iOS operating system currently dominates 59% of mobile device usage in the United States.[32] With an annual revenue of $274.5 billion, Apple, Inc. has proven that a business model for mobile devices can be widely successful without selling consumer information to third parties.[33]

[28] *See* Andrews, *supra* note 27, at 434–36; *see also* Patrick Gage Kelley et al., A "Nutrition Label" for Privacy 1 (July 15, 2020) (unpublished manuscript) (on file with Carnegie Mellon University School of Computer Science), https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf [https://perma.cc/MP2D-S5BN].

[29] *See* Andrews, *supra* note 27, at 435.

[30] *See* discussion *infra* Section V.B.1; *see also* discussion *infra* Section III.A.3 (describing how the CPBR called for transparency, defined as the "right to easily understandable and accessible information about privacy and security practices").

[31] Joseph Johnson, *Digital population in the United States as of January 2021*, STATISTA (Sept. 7, 2021), https://www.statista.com/statistics/1044012/usa-digital-platform-audience/ [https://perma.cc/TJ23-FXSG].

[32] *Mobile Operating System Market Share United States of America*, STATCOUNTER, https://gs.statcounter.com/os-market-share/mobile/united-states-of-america [https://perma.cc/CVT8-2JHP].

[33] *See* Lionel Sujay Vailshery, *Global revenue of Apple from 2004 to 2021*, STATISTA (Nov. 22, 2021), https://www.statista.com/statistics/265125/total-net-sales-of-apple-since-2004/ [https://perma.cc/2AT3-SH68].

[8] In 2021, Apple's iOS 14.5 update[34] introduced its new "App Tracking Transparency" policy.[35] This policy requires each application to present consumers with a clear and simple prompt that asks the consumer if they want their personal information to be tracked and sold by that application. The fact that only 15% of users affirmatively opted in to the tracking and selling of their personal information demonstrates that United States consumers value their privacy and do not want their data to be shared.[36] Apple is unique as the vast majority of businesses do not offer consumers the opportunity to choose whether their information is shared. Absent comprehensive federal privacy law, the majority of websites will continue to track and sell consumer data.

[9] United States privacy law has historically failed to keep up with advances in technology.[37] In 2021, the need for a comprehensive federal privacy law has never been stronger, with widespread use of the internet, smartphones, and everyday items increasingly tracking our every move.[38]

---

[34] *See Update Your iPhone, iPad or iPod Touch*, APPLE (Sept. 23, 2021), https://support.apple.com/en-gb/HT204204 [https://perma.cc/CUK9-A5TR] (explaining how Apple mobile devices run the iOS operating system and that Apple periodically releases updates that make changes to the iOS system, improving its operability and security); *see also iOS 14.5 delivers Unlock iPhone with Apple Watch, more diverse Siri voice options, and new privacy controls*, APPLE (Apr. 26, 2021), https://www.apple.com/uk/newsroom/2021/04/ios-14-5-offers-unlock-iphone-with-apple-watch-diverse-siri-voices-and-more/ [https://perma.cc/TF56-F3L7] [hereinafter *iOS Update*].

[35] *See iOS Update*, *supra* note 34.

[36] *See* Estelle Laziuk, *iOS 14.5 Opt-in Rate - Weekly Updates Since Launch*, FLURRY (Sept. 6, 2021), https://www.flurry.com/blog/ios-14-5-opt-in-rate-idfa-app-tracking-transparency-weekly/ [https://perma.cc/7STA-N4S5].

[37] *See* Kiran K. Jeevanjee, Comment, *Nice Thought, Poor Execution: Why the Dormant Commerce Clause Precludes California's CCPA from Setting National Privacy Law*, 70 AM. U. L. REV. F. 75, 130 (2020).

[38] *See* WHITE HOUSE PRIVACY REPORT, *supra* note 13 (introductory statement of President Barack Obama); *see also* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 774 (2020) (describing how "manufacturers of toasters, toothbrushes, and sex toys are wiring up everything to the Internet of Things").

At the beginning of his administration, President Biden vowed to tackle the lack of federal privacy law. While bipartisan support exists in Congress,[39] the devil is in the details. Congress has spent the past decade debating provisions like a private right of action or federal preemption with repeated witness testimony.[40] For example, Facebook's founder Mark Zuckerberg, has testified to Congress many times, including facts that have been successfully refuted by media sources, only adding to the confusion.[41] Frustrated with the lack of federal law, many states have taken it on themselves to propose, and in some instances, pass privacy laws of their own.[42] This all surrounds a simple question: do United States consumers want to be tracked and have their personal information sold to third parties? The consumer response to the iOS 14.5 update overwhelmingly suggests that the answer to that question is no, with only 15% of consumers affirmatively opting in to personal information sharing.[43]

[39] *See* Cameron F. Kerry, *Will this new Congress be the one to pass data privacy legislation?*, BROOKINGS INST. (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/ [https://perma.cc/RRZ7-G84M].

[40] *See* Olivia Solon, *Fact-checking Mark Zuckerberg's testimony about facebook privacy*, GUARDIAN (Apr. 11, 2018, 7:13 PM), https://www.theguardian.com/technology/2018/apr/11/fact-checking-mark-zuckerberg-testimony-congress [https://perma.cc/G25N-NGMQ]; Jessica Rich, *After 20 years of debate, it's time for Congress to finally pass a baseline privacy law*, BROOKINGS INST. (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ [https://perma.cc/2PNK-K5FN]; *see also* Salvador Rodriguez, *Senators demand Facebook CEO Mark Zuckerberg answer questions after whistleblower's revelations at hearing*, CNBC, LLC (Oct. 5, 2021, 6:33 PM). https://www.cnbc.com/2021/10/05/congress-demands-mark-zuckerberg-answer-questions-at-haugen-hearing.html [https://perma.cc/9D9M-Q6WW].

[41] *See* Solon, *supra* note 40; *see also* Rodriguez, *supra* note 40.

[42] *See, e.g.*, discussion *infra* Section IV.B–D.

[43] *See* Laziuk, *supra* note 36.

[10] The current patchwork of sectoral and state-specific laws in the United States is difficult to follow as many provisions are vague and interpreted multiple ways.[44] The trend in state-enacted privacy laws, beginning with the California Consumer Privacy Act (CCPA), and now across the Virginia Consumer Data Protection Act (VCDPA) and the Colorado Privacy Act (CPA), is turning away from pro-consumer features supported by the FIPPs and the CPBR formats.[45] These state laws rely on the pro-business format of opt-out consent and regulation by the state attorneys general, instead of the opt-in consent model and private rights of action that favor consumers.[46] The opt-out consent model likely does not protect the majority of consumers that may not have the time, sophistication, or education level to understand and initiate the opt-out process for each of the thousands of websites they click on each year.

[11] As Colorado State Senator Robert Rodriguez explained, "young people assume they have no privacy and old people have no idea how much privacy they don't have."[47] Without a private right of action, businesses are essentially free to continue the tracking and sharing of consumers' personal information until a federal agency initiates an action against them. This relaxed form of regulation further exemplifies the need for strong federal privacy law.

---

[44] *See* discussion *infra* Section VI.A (explaining the CCPA's service provider exception has been interpreted by Facebook to mean the CCPA does not apply to it.); *see* discussion *infra* Section IV.C (stating the VCDPA's affiliate exception is another example that is subject to interpretation)*; see also* Andrews, *supra* note 27, at 435 (explaining how businesses often categorize affiliates as any third party willing to pay for the consumer's data).

[45] *See* discussion *infra* Section IV.B; *see* discussion *infra* Section IV.C; *see* discussion *infra* Section IV.D.

[46] *See* discussion *infra* Section IV.B; *see* discussion *infra* Section IV.C; *see* discussion *infra* Section IV.D.

[47] Saja Hindi, *Colorado Lawmakers Advance Data Privacy Legislation*, DENVER POST (June 1, 2021), https://www.govtech.com/policy/colorado-lawmakers-advance-data-privacy-legislation [https://perma.cc/WWU9-2C2Z].

[12] This article argues that Congress should draw from the principles of the GDPR, the iOS 14.5 update, and certain features of state privacy laws to enact federal privacy legislation that (1) applies to all businesses that collect personal information from consumers located in the United States, (2) requires consumers to provide affirmative opt-in consent for data tracking and sharing, and (3) provides for a private right of action to put an end to the illicit surveillance and data exploitation that continues to run rampant. The iOS 14.5 update has demonstrated that when faced with a simple, comprehensible choice to opt in to the tracking and sharing of their personal information, few consumers in the United States consent.[48] Apple's iOS results illustrate the United States consumers' thirst for privacy and the palpable need for federal privacy regulation of all entities handling such data. Left virtually unregulated, many online applications and websites track and share consumer personal data without their knowledge or consent.[49] This practice subjects individuals to potential privacy harms, such as social stigmatization, reputational damage, discrimination, and safety concerns.[50] Thus, a federal law is needed to prohibit businesses from sharing the personal data of unsuspecting consumers for valuable consideration, absent affirmative opt-in consent.

[13] This article utilizes a Privacy Spectrum to illustrate the impact of privacy laws. On the strong end of the spectrum, there is a high level of consumer protection with a low potential of consumer harm. On the weak end, there is a low level of consumer protection with a high potential of consumer harm.

[48] *See* Laziuk, *supra* note 36.

[49] *See* Confessore, *supra* note 4.

[50] *See* discussion *infra* Section II.

[14] The stars have aligned for federal privacy legislation with the change in administration,[51] iOS 14.5 update data,[52] examples of state privacy laws to discern what is helpful or not helpful,[53] and the technology industry itself calling for federal legislation.[54] It is time for Congress to protect consumer personal privacy. This article proposes guidelines for Congress when enacting federal privacy legislation. Section II provides a brief introduction to consumer privacy harms. Section III introduces the historical background of privacy law in the United States and provides an overview of current privacy law. Section IV provides a summary of the General Data Protection Regulation (GDPR) and three recently enacted state laws that are referenced when recommending federal privacy law. Section V identifies the iOS 14.5 update data and its influence while analyzing key components necessary for consumer privacy protection at the federal level. Section VI proposes five key elements to be utilized in effectively implementing federal privacy law. Section VII summarizes how to integrate the iOS 14.5 update's current consumer data with features of existing law to stop the surveillance and tracking that currently affects all Americans.

[51] *See* Colin Rahill, *The State of Privacy under a Biden Administration: Federal Cybersecurity Legislation, Strict Regulatory Enforcement, and a New Privacy Shield with the EU*, HARV. J.L. TECH. DIG. (Feb. 20, 2021), http://jolt.law.harvard.edu/digest/the-state-of-privacy-under-a-biden-administration-federal-cybersecurity-legislation-strict-regulatory-enforcement-and-a-new-privacy-shield-with-the-eu [https://perma.cc/8922-TKV5].

[52] *See* discussion *infra* Section V.B.2.

[53] *See* discussion *infra* Section IV.

[54] *See* Jon Berroya, *Congress Must Act to Protect Americans' Privacy*, REALCLEAR POL'Y (June 4, 2020), https://www.realclearpolicy.com/articles/2020/06/04/congress_must_act_to_protect_americans_privacy_495194.html [https://perma.cc/N5N6-5QQ8] (calling for comprehensive federal data privacy legislation by the CEO and President of Internet Association).

II. PRIVACY HARMS

[15] Consumer privacy issues encroach on a variety of different scenarios, ranging from discrimination to economic loss to emotional impairment.[55] For example, the disclosure of personal data may affect a consumer's ability to obtain insurance, housing, employment, financial products, or admission to a nursing home; it may cause social stigmatization based on disease, mental health conditions, addictions, race, sexual preferences, political opinions, or religion; it may subject the consumer to unfair business practices and unwanted fraudulent offers; and it may subject the consumer to potentially dangerous situations due to the revelation of secret locations for domestic abuse victims or persons in witness protection programs, bullying, stalking, Ransomware, or blackmail.[56] This section will address the most pertinent of the potential harms: discrimination, social stigmatization, and physical safety.

[16] Discrimination occurs in the employment, insurance, housing, and banking industries based on a consumer's health information.[57] While the Americans with Disabilities Act of 1990 prohibits potential employers from "obtaining medical information about applicants before offering employment,"[58] employers still discriminate against individuals with preexisting health conditions for job offers and promotions.[59] Insurance companies regularly obtain data from other entities and factor it into coverage determinations.[60] This may result in assigning customers higher

[55] *See* Determann, *supra* note 26.

[56] *Id.*; *see also* Andrews, *supra* note 27, at 465-66.

[57] *See* Determann, *supra* note 26 at 256, 258.

[58] Andrews, *supra* note 27, at 465.

[59] Determann, *supra* note 26, at 229, 258 ("Employers could use health information as an opportunity to assess the performance of their employees or to refrain from hiring, retaining, or promoting job candidates.").

[60] *See id.* at 229.

rates for health, life, or disability insurance or refusing to insure them at all.[61] "For example, a consulting group advises life insurers to deny insurance or charge more if the person eats fast food, commutes to work, is an avid reader, or who has friends who are skydivers."[62] Banks may refuse to grant loans or credit cards[63] to those they consider unhealthy because "one without serious diseases is more likely to work longer and therefore to be able to meet his or her contractual obligations."[64] In the housing industry, healthy tenants can be viewed as more reliable than those with a medical condition.[65]

[17] The disclosure of an individual's personal information often creates a negative stigma in social settings.[66] Addictions like drug and alcohol abuse or mental health conditions, along with certain diagnoses, such as COVID-19, sexually transmitted disease, prescription drug use, or mental health issues, carry additional stigmatizations.[67]

[18] Further stigmatization can occur when online accounts make their way into the consumers' real lives. Facebook has positioned itself to be a

[61] *Id.* at 258.

[62] Andrews, *supra* note 27, at 431.

[63] *Id.* at 466.

[64] Determann, *supra* note 26, at 258.

[65] *Id.*

[66] *Id.* at 229–30.

[67] *See* Müge Fazlioglu, *Privacy Risks to Individuals in the Wake of COVID-19*, INT'L ASS'N PRIV. PROF'LS, June 2020, at 1, 3 (noting that patients diagnosed with COVID-19 can become "subjects of avoidance or exclusion from economic or social life," and that COVID-19 positive individuals have been "socially ostracized, doxed, or threatened"); *see also* Determann, *supra* note 26, at 256–57 (explaining that when faced with a mental health diagnosis, patients may experience "embarrassment, shame, and even social exclusion should information of this nature become public," and that this stigmatization often affects an individual's quality of life and can cause additional health conditions or a variety of psychosomatic symptoms.).

gatekeeper for law enforcement, searching for individuals whose online activities may infer suicidal tendencies.[68] Facebook scans users' input—including private messages—for content that may apply to safety and health.[69] Facebook uses this information to report individuals they consider as potentially suicidal to law enforcement.[70] Thus, by utilizing Facebook, a user runs the risk of the police showing up at their door in real life if Facebook determines they are a suicide risk.[71] This can be particularly troubling when police documentation of such a visit becomes a public record, which may be shared with any interested parties—including data brokers.[72]

[19] The physical safety of consumers may be compromised when personal data is disclosed.[73] Breaches of privacy may increase the risk of bullying, stalking, or blackmail incidents. The revelation of secret locations for domestic abuse victims or persons in witness protection programs can create dangerous situations.[74] For example, a private investigator located

[68] *See* Benjamin Goggin, *Inside Facebook's suicide algorithm: Here's how the company uses artificial intelligence to predict your mental state from your posts*, BUS. INSIDER (Jan. 6, 2019, 11:19 AM), https://www.businessinsider.com/facebook-is-using-ai-to-try-to-predict-if-youre-suicidal-2018-12 [https://perma.cc/H4KJ-TP5X].

[69] *See* Mason Marks, *Artificial Intelligence–Based Suicide Prediction*, 21 YALE J.L. & TECH. 98, 108 (2019).

[70] *See* Goggin, *supra* note 68.

[71] *Id.*

[72] *See FOIA How To*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/transparency/foia-how-to [https://perma.cc/L76V-6KFJ].

[73] *See* Determann, *supra* note 26, at 256.

[74] *See id.* at 256–58 (explaining how blackmail can result when medical data falls into the wrong hands and implies something a patient may prefer to keep a secret, such as sexual orientation).

the home address of an actress, Rebecca Schaefer, through California motor vehicle records.[75] A stalker utilized the home address to murder Schaefer.[76]

III. THE EVOLUTION OF PRIVACY LAW

[20] Americans possess a Constitutional right to privacy, implied by the Fourth Amendment.[77] This right was further defined by Supreme Court cases that provided consumers with privacy rights in their own person[78] and the freedom to move about in public spaces without their every movement being tracked and recorded.[79] While strong indicators of a consumer's right to privacy, these laws and decisions only apply to government actors and were made during a time when technology was far less pervasive (and invasive) than it is today.[80] Absent federal privacy legislation that addresses the current technological trends, consumers are left vulnerable to exploitation from private parties—such as data brokers and advertising schemes.[81] Understanding the need for federal privacy legislation requires understanding the history of privacy laws in the United States, as well as the virtues and shortcomings of current privacy oversight. This Section will

[75] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV., (forthcoming 2022) (manuscript at 19).

[76] *Id.*

[77] Michael Goodyear, *The Dark Side of Videoconferencing: The Privacy Tribulations of Zoom and the Fragmented State of U.S. Data Privacy Law*, 10 HOUS. L. REV. 76, 81 (2020).

[78] *See* Katz v. United States, 389 U.S. 347, 358–59 (1967).

[79] *See* United States v. Jones, 132 U.S. 945, 955–57 (2012).

[80] *See Katz*, 389 U.S. at 358 (holding only applying to government actors and this case was decided in 1967, prior to the internet.); *see also Jones*, 132 U.S. at 955–57 (holding only applying to government actors and this case was decided in 2012, before many of the more invasive surveillance and tracking methods were implemented to monitor an internet users' every move)

[81] *See What Are Data* Brokers, *supra* note 1.

discuss the history of privacy law in the United States and provide an outline of the existing privacy laws.

A. History of Privacy Law and Discourse in the United States

[21] In 1890, Louis Brandeis and Samuel Warren published *The Right to Privacy*, a famous law review article that defined an individual's right to privacy and recognized their right to be left alone.[82] This basic set of rights eventually led to the privacy torts we have today, designed to protect individuals from privacy harms.[83] Brandeis and Warren opined that "[i]f the invasion of privacy constitutes a legal *injuria*, the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."[84] Thus, a private right of action for privacy torts was born, allowing individuals the right to recovery.[85] These original rights of privacy are still the subject of extensive testimony and debate, as Congress has failed to pass a comprehensive federal privacy law.[86] This section will discuss (1) the Fair Information Practice Principles and The Privacy Act, (2) the FTC's call for privacy regulation, (3) the Consumer Privacy Bill of Rights, (4) California voter initiatives, and (5) Congressional privacy debates.

[82] *See* Samuel D. Warren & Louis D. Brandeis, *Right to Privacy*, 4 HARV. L. REV. 193, 194–96 (1890–91).

[83] *See id*. at 193, 195 (introducing the right to be let alone); *see also* RUSSELL L. WEAVER ET AL., MASTERING TORT LAW 286 (2nd ed. 2016) (stating that the four invasion of privacy torts recognized today in most jurisdictions are Appropriation, Intrusion on Seclusion, Publication Disclosure of Private Facts, and False Light).

[84] *See* Warren & Brandeis, *supra* note 82, at 213.

[85] *See id.* at 213–15, 219.

[86] *See* Solon, *supra* note 40.

1. Fair Information Practice Principles and The Privacy Act—1973–74

[22] In 1973, the Fair Information Practice Principles (FIPPs) were derived from *Records, Computers, and the Rights of Citizens*, a report issued by the Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems.[87] The FIPPs are considered the "Gold Standard" of consumer personal information protection[88] and "have been employed in many 'different formulations coming from different countries and different sources over the decades.'"[89] The FIPPs recommend the following as best practices: (1) not utilizing personal record-keeping systems that are kept secret; (2) providing a process for individuals to discover any information about them contained in a record and how it is used; (3) providing a process for individuals to prevent information about them from being made available or used for other purposes than the reason it was obtained without the individual's consent; and (4) providing individuals with a process to amend or correct a record containing identifiable information about them.[90]

[23] The FIPPs still reverberate today in various federal and state legislative efforts,[91] with an emphasis on data quality, use limitation, openness, accountability, collection limitation, purpose specification, security safeguards, and individual participation.[92] These principles are on

[87] *See* Andrew Proia et al., *Consumer Cloud Robotics and the Fair Information Practice Principles: Recognizing the Challenges and Opportunities Ahead*, 16 MINN. J.L. SCI. & TECH. 145, 159 (2015).

[88] *Id.* at 158.

[89] *Id*. at 160 (internal citations omitted).

[90] *See id.* at 159 n.70.

[91] *See id*. at 160 (describing the FIPPs as "basic principles which can be built into existing national legislation").

[92] *See* Proia et al., *supra* note 87, at 160.

the strong end of the Privacy Spectrum and clearly intend to provide consumers more protection with less harm.

[24] The Privacy Act of 1974 outlined its own fair information practices that focused on an individual's right to notice and consent before their personal information could be collected and utilized, along with access to and security of their data.[93] While the Act only applied to personally identifiable information contained in federal agency records, it provided a baseline for privacy law in the United States that is still recognized today.[94]

2. The FTC's Call for Privacy Regulation—2000

[25] In 2000, "a few years after the internet became an everyday medium, four years before Facebook was created, and seven years before the iPhone would be introduced," the FTC called on Congress to pass a federal law to protect the privacy rights of Americans.[95] This need was clear, "even before we had mobile devices, social networks, apps, and detailed tracking of our every movement and location."[96] The FTC proposed that every online company must provide consumers with the choice of how their data could be used beyond the original purpose for which the data was provided.[97] Congress did not enact legislation based on this FTC proposal.[98]

[26] In the decades that followed, the FTC has brought "legal actions against organizations that have violated consumers' privacy rights, or

[93] *See* Privacy Act of 1974, 5 U.S.C. § 552a (describing the Act as having "establishe[d] a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies").

[94] *See id.*

[95] *See* Rich, *supra* note 40.

[96] *Id.*

[97] *Id.*

[98] *Id.*

misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury."[99] The FTC often charges defendants with violating Section 5 of the FTC Act, "which bars unfair and deceptive acts and practices in or affecting commerce."[100]

3. The Consumer Privacy Bill of Rights Proposal—2012

[27] In 2012, the White House created the Consumer Privacy Bill of Rights (CPBR) as a blueprint for Congress to develop legislation and for stakeholders to develop codes of conduct.[101] It was a simple, comprehensive plan to protect consumer privacy that highlighted the basic points for which privacy advocates are still fighting almost a decade later.[102] The CPBR featured principles at the strong end of the Privacy Spectrum that provide consumers more protection with less risk of harm.

[28] The Obama Administration believed the FIPPs were "the widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy."[103] The CPBR applied the globally recognized FIPPs to "an environment in which processing of data about individuals is far more decentralized and pervasive than it was when FIPPs were initially

[99] *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/T534-A5AP].

[100] *Id.*

[101] *See generally* WHITE HOUSE PRIVACY REPORT, *supra* note 13 (introductory statement of President Barack Obama).

[102] *See* WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 1–2.

[103] THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY 45 (2011); WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 9 (describing how FIPPs were the basis for the CPBR).

developed."[104] While sufficient for the CPBR, some privacy advocates have been critical of the FIPPs for not being strong enough to protect consumers from advances in technology.[105]

[29] The CPBR focused on providing "consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data."[106] The CPBR was divided into seven objectives: (1) Individual Control, (2) Transparency, (3) Respect for Context, (4) Security, (5) Access and Accuracy, (6) Focused Collection, and (7) Accountability to protect commercial uses of personal data that included any data "linkable to a specific individual."[107]

[30] The Individual Control element is reflected in today's opt-in consent model.[108] This principle establishes that consumer-facing companies should provide consumers with choices about the personal data the company collects.[109] It encourages companies to "seek ways to recognize consumer choices through mechanisms that are simple, persistent, and scalable from the consumer's perspective."[110] This principle is exemplified in the iOS 14.5 update; it asks the user if they want to be tracked. The iOS format is also persistent and can easily be replicated across devices.

---

[104] WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 9.

[105] *See* Proia et al., *supra* note 87, at 180 (discussing practical challenges of applying the FIPPs to advanced robotic technology), 202 (identifying how modern technologies struggle with providing proper disclosures), 206 (providing an example where accountability is becoming "increasingly difficult given the external pressure for increased flexibility in design of rules").

[106] WHITE HOUSE PRIVACY REPORT, *supra* note 13 (introductory statement of President Barack Obama).

[107] *Id.* at 1, 10.

[108] *See id.* at 11.

[109] *See id.*

[110] *Id.*

[31] The Focused Collection element asserts that "[c]onsumers have a right to reasonable limits on the personal data that companies collect and retain."[111] Under this element, data should only be collected when needed to accomplish its disclosed purposes, with businesses securely disposing or de-identifying it once it is no longer necessary, unless legally prohibited.[112] Had this belief been incorporated into federal privacy law a decade ago, the United States would likely not be in the position where large companies know everything about individuals' daily activities.

[32] The Transparency element asserts that companies should provide clear enough descriptions for consumers to understand how their personal data is shared.[113] It recommends that statements be provided to consumers regarding their ability to exercise individual control when they are "most relevant to understanding privacy risks and easily accessible when called for."[114] More prominent disclosures are needed when personal data is utilized for purposes that are inconsistent with the context or relationship between the company and consumer.[115] Transparency is again one of the core principles that privacy advocates are still fighting for in the push for federal privacy legislation.[116]

[33] In 2013, a National Security Administration (NSA) scandal broke that tested the principles of the CPBR. Edward Snowden revealed that the NSA had "collected hundreds of thousands of user address books from email providers and even hacked into the private networks that companies

[111] WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 21.

[112] *Id.*

[113] *Id.* at 14.

[114] *Id.*

[115] *Id.*

[116] *See* Kerry, *supra* note 39; *see also* Letter from Elec. Priv. Info. Ctr. et al., to John Thune, Chairman, U.S. Senate Comm. on Com., Sci., & Transp., et al. (Oct. 9, 2018), https://epic.org/testimony/congress/CPOs_to_SCC_US_Data_Protection_Framework_Oct2018.pdf [https://perma.cc/3XTS-2BUQ] [hereinafter Letter from EPIC].

like Google and Yahoo use to transport their data."[117] The NSA "was collecting rivers of personal data—emails, photos, instant-message conversations—from nine leading internet companies, including Google, Facebook, Yahoo and Microsoft."[118] According to Ashkan Soltani,[119] a former technologist who worked on Google and Facebook privacy investigations at the FTC, these revelations damaged the Administration's moral authority as consumers learned the government itself had been illicitly spying on their online interactions.[120]

[34] Big Tech firms began meeting with the Administration, outraged by the allegations, while advocating for their own pro-business agendas.[121] These agendas directly conflicted with privacy regulation designed to strengthen consumer privacy rights.[122] In 2014, Penny Pritzker, the co-chair of Obama's re-election campaign, traveled to Silicon Valley to meet with eBay, Google, and Sheryl Sandberg at Facebook.[123] Pritzker and Sandberg discussed "consumer privacy and how to ensure that American tech businesses remained competitive around the world."[124] Pritzker "hailed the tech industry as a model for government—a partner, not an antagonist. Data, she proclaimed, was 'the fuel of the 21st century.'"[125] By 2015, a watered-down version of the CPBR contained so many pro-business exceptions and

[117] Confessore, *supra* note 4.

[118] *Id.*

[119] *See id.*

[120] *See id.*

[121] *See id.*

[122] Confessore, *supra* note 4.

[123] *Id.*

[124] *Id.*

[125] *Id.*

carve-outs that "[consumer advocates] were furious."[126] Ultimately, the White House's original foundation for consumer privacy was dead in the water.[127] The need for privacy protection, as illustrated in the initial principles of the CPBR, still exists today. Nearly a decade later, privacy advocates continue to push for federal legislation echoing these basic principles.

4. California Voter Initiatives—2018

[35] In 2018, with no federal privacy law in sight, the CCPA was hastily passed as a compromise between the legislature, Big Tech, and Californians for Consumer Privacy (CFCP)—an organization led by real estate investor Alastair Mactaggart.[128] Mactaggart accidentally stumbled on this passion for consumer privacy while dining with a software engineer from Google.[129] When Mactaggart asked the engineer if consumers should be concerned about the large quantities of information Google knows about them, the engineer said " . . . there was plenty to worry about. If people really knew what we had on them . . . they would flip out."[130] This conversation sparked Mactaggart's research on data mining and online tracking, eventually leading to the creation of CFCP and two privacy initiatives.[131]

[36] Mactaggart amassed the necessary 629,000 signatures to qualify CFCP's initiative for the California statewide elections in November

[126] *Id.*

[127] Confessore, *supra* note 4.

[128] *Id.*; *California Privacy Rights Act Executive Summary*, CALIFORNIANS FOR CONSUMER PRIV., https://www.caprivacy.org/cpra-exec-summary/ [https://perma.cc/TT3J-UCRQ] [hereinafter *CPRA Executive Summary*] (describing Mactaggart as CFCP's leader).

[129] Confessore, *supra* note 4.

[130] *Id.*

[131] *Id.*; *see also CPRA Executive Summary*, *supra* note 128.

2018.[132] Big tech companies, including Google, Verizon, AT&T, Facebook, and Comcast, heavily opposed the initiative, deeming it unworkable and claiming they were prepared to spend an estimated $100 million to fight it.[133] Coincidentally, news of Facebook's Cambridge Analytica scandal broke out prior to the election, positioning it as the focus of "a legal, political, public relations, and media nightmare."[134] Facebook admitted that Cambridge Analytica had obtained access to the personal information of up to 87 million Facebook users,[135] and "coerce[d] voters through 'deploying powerful "psychographic" voter profiles'" by utilizing voters' own Facebook data.[136] The timing of the scandal pushed the lack of privacy regulation into the spotlight and tipped the scales in favor of the initiative.[137]

[37] In subsequent negotiations with lawmakers and Big Tech, Mactaggart agreed to withdraw the initiative if the legislature passed a "reasonable privacy bill by June 28, [2018,] the legal point of no return for formally withdrawing [the] initiative."[138] Many California legislators declined to "upset their tech-based financiers" while Big Tech adamantly refused a bill containing private rights of action.[139] On June 26, 2018, Big Tech ultimately agreed to back the CCPA because it "'prevent[ed] the even-

[132] Confessore, *supra* note 4.

[133] *Id.*

[134] Jordan Yallen, *Untangling the Privacy Law Web: Why the California Consumer Privacy Act Furthers the Need for Federal Preemptive Legislation*, 53 LOY. L.A. L. REV. 787, 793 (2020).

[135] Confessore, *supra* note 4.

[136] Yallen, *supra* note 134.

[137] *Id.*

[138] *Id.*

[139] *Id.* at 794.

worse ballot initiative from becoming law,' bought the industry time, and was amendable."[140]

[38] While the CCPA went into effect in 2020, government agencies, Congress, and Big Tech have pushed for federal legislation to preempt the act.[141] These entities fear that more states will implement their own privacy statutes, potentially disrupting business and innovation by forcing companies to comply with fifty unique laws.[142]

[39] The efforts of Mactaggart's organization lead to another voters' initiative that amended the CCPA,[143] further strengthening consumers' rights.[144] The California Privacy Rights Act of 2020 (CPRA) was approved as a ballot initiative by a majority of voters in the November 2020 general election.[145] Because the CPRA was a ballot initiative, it cannot be repealed by the state legislature and can only be amended with requirements that further the intent and purpose of the Act.[146]

[140] *Id.* at 795 (internal citations omitted).

[141] Guynn, *supra* note 5.

[142] *Id.*

[143] *CPRA Executive Summary*, *supra* note 128.

[144] *See id.* (noting that the CPRA amended the CCPA to eliminate the 30 day right to cure provision that allowed a business 30 days to revise its practices after a violation notice was issued).

[145] *See id.* (noting that the CPRA takes effect in 2023).

[146] *The gathering storm: Proposition 24 and the future of US privacy*, MEDIUM (Aug. 16, 2020), https://medium.com/golden-data/the-gathering-storm-proposition-24-and-the-future-of-us-privacy-b27d1deb8d90 [https://perma.cc/AK2Z-JQEN].

5. Congressional Privacy Debates

[40] As Congress has continued to debate potential privacy law since the FTC made its recommendation in 2000, little progress has been made. According to Cameron F. Kerry, who worked with the Obama administration in drafting legislation based on the CPBR, there is a lot of agreement on essential principles of privacy law. [147] Kerry observed that "it is a challenge to articulate these [principles] in ways that are concrete without being too prescriptive or too narrow."[148]

[41] In 2018, Senator John Thune stated there was strong bipartisan support to develop a federal privacy law and "the question is no longer whether we need a federal law to protect consumers' privacy. The question is what shape it should take."[149] A wide variety of stakeholders, such as the Electronic Privacy Information Center, Google, the Internet Association, and the United States Chamber of Commerce, have issued principles or frameworks regarding the privacy aspects legislation should address.[150] Even with the growing push for federal privacy legislation, Congress has failed to agree on pertinent issues such as private rights of action and state law preemption, thus continuing to leave consumers unprotected.[151]

[42] In 2019, fifty-one chief executive officers of Big Tech firms signed an open letter to Congress calling for "a comprehensive consumer data privacy law that strengthens protections for consumers and establishes a national privacy framework to enable continued innovation and growth in

[147] Kerry, *supra* note 39.

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] Rahill, *supra* note 51.

the digital economy."[152] Members of both political parties in the 2019 Legislature expressed a desire to pass federal privacy legislation after the Cambridge Analytica scandal, passage of the CCPA, and the GDPR.[153] The debate on Capitol Hill included three main issues: (1) whether a federal privacy law should preempt tougher state privacy laws, such as the CCPA; (2) whether consumers should have a private right of action over privacy violations; and (3) whether the Federal Trade Commission (FTC) should be the enforcement agent to oversee corporate privacy practices.[154]

[43] The National Telecommunications and Information Administration, under the Trump Administration, collected hundreds of comments from the public and businesses potentially impacted by privacy legislation.[155] In the end, the Trump White House did not produce a roadmap to protect consumer data, with President Donald Trump focused instead on complaints about tech companies that "are biased against conservatives."[156]

[44] The Information Transparency & Personal Data Control Act was introduced to Congress in 2019, proposing the requirement for affirmative opt-in consent by consumers for use of their data.[157] Congress did not pass

[152] Letter from Randall Stephenson, Chairman & CEO, AT&T Inc., et al. to Mitch McConnell, Majority Leader, U.S. Senate, et al. (Sept. 10, 2019) (on file with Business Roundtable).

[153] *See* Hendel, *supra* note 17; *see also* Directive 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 and on the free movement of such data, and repealing Directive 95/46/EC, 2016 O.J. (L 679) 1 [hereinafter GDPR] (demonstrating how the GDPR is a comprehensive privacy law designed to prohibit businesses from tracking and selling the personal information of consumers located in the EU, absent consent).

[154] *See* Hendel, *supra* note 17.

[155] *Id.*

[156] *Id.*

[157] *See* Information Transparency & Personal Data Control Act, H.R. 2013, 116th Cong. (2019).

this bill.[158] Even if the bill had been enacted into law, it would have transferred the responsibility back to the FTC to establish the actual regulation.[159]

[45] In 2021, Big Tech has placed support behind the VCDPA and is calling on Congress to model federal legislation after its less restrictive, pro-business format.[160] The VCDPA only applies to a narrow scope of large entities, utilizes the opt-out consent model, and does not provide for a private right of action.[161] The Internet Association[162] has positioned itself as pro-legislation, while calling for the inclusion of data brokers and brick and mortar retailers into any privacy regulation.[163]

[46] While decades have passed since the FTC called on Congress for privacy legislation, entire industries have been developed around the tracking and sharing of consumers' personal information absent the consumers' affirmative consent. As Jessica Rich, former Director of Consumer Protection at the FTC, stated, "the intervening years have brought us massive data breaches, virtually unlimited data collection online and in our public spaces, huge platforms that know everything about us and

[158] *See id.*

[159] *Id.*

[160] *See* Hayley Tsukayama, *Virginia's Weak Privacy Bill Is Just What Big Tech Wants*, ELEC. FRONTIER FOUND. (Feb. 25, 2021), https://www.eff.org/deeplinks/2021/02/virginias-weak-privacy-bill-just-what-big-tech-wants [https://perma.cc/GE7Z-AUAY].

[161] *See* discussion *infra* Section IV.C.

[162] *See generally Members*, INTERNET ASS'N, https://internetassociation.org/our-members/ [https://perma.cc/8XQB-478N] (showing that the Internet Association is an internet lobbying group, formed by several companies, including Google, Facebook, eBay, and Amazon and claiming to be "the only trade association that exclusively represents leading global internet companies on matters of public policy").

[163] *See* Berroya, *supra* note 54.

dominate the marketplace, and algorithmic predictions that create risk of bias and loss of opportunity."[164]

B. Current Patchwork of Privacy Law in the United States

[47] Absent comprehensive federal privacy law, the United States currently relies on data privacy regulation in specific industries, at the state level, through private tort claims, or by the FTC when a particular act is considered "unfair or deceptive."[165] A tangled web of federal and state laws exists[166] that makes identifying and complying with consent and information exchange laws a difficult undertaking.[167]

[48] All consumers are affected by the harms that federal regulation would address, whether they use the internet or not.[168] Big Tech's model of consumer privacy is described as one that "puts the onus on the user to decide if the bargain is fair . . . It's like selling you coffee and making it your job to decide if the coffee has lead in it . . . [W]e have no baseline law that says you can't put lead in coffee."[169]

[49] As of this writing, bipartisan support exists from Congress and the Biden Administration to pass a comprehensive privacy law.[170] Vice President Kamala Harris brings a strong track record in privacy enforcement

[164] Rich, *supra* note 40.

[165] *See* Goodyear, *supra* note 77, at 81–82.

[166] *See id.* at 86.

[167] *See id.* at 81–83.

[168] *Cf. What Are Data* Brokers, *supra* note 1 (detailing how data brokers collect information from non-Internet sources, like information linked to consumers' store loyalty cards).

[169] Confessore, *supra* note 4.

[170] *See* Rahill, *supra* note 51.

to the Administration from her time as California Attorney General.[171] Harris negotiated with Big Tech to agree on some standards that strengthened consumer privacy and was integral in requiring tech startups to hire a Chief Privacy Officer.[172] A variety of Obama staffers that contributed to the formation of the Federal Privacy Council and the CPBR have returned to the Biden administration.[173] President Biden announced his administration is "elevat[ing] the status of cyber issues."[174] Biden is pushing the FTC for "more aggressive enforcement of privacy regulations and antitrust action" as it has ongoing investigations regarding the data collection practices at YouTube, Amazon, Twitter, and Facebook.[175]

[50] In April 2021, a Morning Consult study showed bipartisan support from voters with 86% of Democrats and 81% of Republicans polling that they favor federal privacy legislation.[176] The study showed that 88–89% of voters want their Social Security number, banking information, and biometric data protected, while 77–81% want their online-specific data, such as geolocation data and internet browsing history, protected.[177]

[171] *See id.* (stating that Harris was involved in the strict privacy amendment to the California Online Privacy Protection Act ("CalOPPA"), which was the first state law requiring commercial websites to include privacy disclosures).

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *See* Rahill, *supra* note 51.

[176] Sam Sabin, *States are Moving on Privacy Bills. Over 4 in 5 Voters Want Congress to Prioritize Protection of Online Data*, MORNING CONSULT (Apr. 27, 2021, 12:01 AM), https://morningconsult.com/2021/04/27/state-privacy-congress-priority-poll/ [https://perma.cc/HC7H-6E8W].

[177] *Id.* (graphing survey results regarding protection of sensitive personal information by specific type of information).

[51] With Democrats controlling the Senate and House in 2021, their Consumer Online Privacy Rights Act (COPRA)[178] is a likely candidate for federal privacy legislation.[179] COPRA would allow consumers to sue for damages under a private right of action and would not preempt state privacy laws if those laws provide stronger requirements.[180] The FTC would receive new resources and capabilities for enforcement by expanding its authority with a new bureau.[181] There is still more work to be done in order to protect consumers' privacy as COPRA generally provides an opt-out consent model, absent certain exceptions.[182] While COPRA is a good start for federal legislation, it should require the opt-in consent model. Opt-in consent provides strong privacy protection because it requires consumers to take affirmative action if they want their personal information to be shared.

[52] While the passage of the GDPR provided strong protections for individuals in the European Union (EU), the passage of the VCDPA and the CPA signal that the United States appears to be moving further away from the pro-consumer model. The VCDPA and the CPA only apply to a narrow scope of businesses, utilize the opt-out consent model, and do not provide a private cause of action.[183] Instead of supporting the opt-in consent model,[184] states are increasingly siding with business backers who want the ability to

[178] *See generally* Consumer Online Privacy Rights Act, S. 2968, 116th Cong. (2019) (actual text of COPRA).

[179] Rahill, *supra* note 51.

[180] *See id.*

[181] *Cf.* S. 2968.

[182] *See id.*

[183] *See* discussion *infra* Section IV.C; *see also* discussion *infra* Section IV.D.

[184] *See* discussion *infra* Section V.B (The opt-in consent model provides consumers with rights to affirmatively consent to the sale of their personal information).

track and sell consumers' data without obtaining informed consent.[185] This trend is weakening consumers' rights on the Privacy Spectrum as it provides for low consumer protection with a high risk of harm.

[53] The struggle between pro-consumer and pro-business provisions over the consumers' right to opt in to the sale of personal information was evident in the 2021 CPA debates. The original bill included the opt-in consent provision.[186] The Senate Business, Labor, and Technology Committee replaced the opt-in provision with the pro-business format of opt-out.[187] The Senate then amended the bill to revert back to opt-in, only to have the House revert back to opt-out right before passing it.[188]

[54] While the federal privacy debates continue, consumers are left with fragmented privacy rights that are difficult to understand and implement. The following section will discuss current privacy law in the United States: (1) United States Constitution and Common Law, (2) Sectoral Privacy Law, (3) Private Tort Claims, (4) FTC Enforcement, and (5) State Privacy Laws.

1. United States Constitution and Common Law

[55] The United States Constitution Bill of Rights contains an implied right of privacy in the Fourth Amendment.[189] An individual's reasonable expectation of privacy is often measured by the standard established in *Katz*

[185] *See* discussion *infra* Section V.B (The CCPA, VCDPA, and the CPA contain opt-out consent models).

[186] *See* David Stauss et al., *Significantly Amended (Again) Colorado Privacy Act Passes Senate*, HUSCH BLACKWELL (May 26, 2021), https://www.bytebacklaw.com/2021/05/significantly-amended-again-colorado-privacy-act-passes-senate/#more-3301 [https://perma.cc/Z5Z5-HJ5F].

[187] *See id.*

[188] *See* S. 190, 2021 Gen. Assemb., Reg. Sess. (Colo. 2021) [hereinafter CPA].

[189] *See* Goodyear, *supra* note 77, at 81.

v. United States.[190] In *Katz,* the Court moved away from only constitutionally protecting one's privacy in physical spaces to protecting the privacy of an individual themselves.[191] This test measures an individual's expectation of privacy by whether it is one that society is prepared to recognize as reasonable.[192]

[56] In *United States v. Jones*, the Court determined that law enforcement should not have immediate access to every move a person makes over an extended period of time without consent or a warrant.[193] The Court held the warrantless placement of a GPS tracking device on a person's vehicle, in order to track all of the movements of a person on public streets, was considered an unlawful search that violated the "effects" portion of the Fourth Amendment.[194] Under *Jones*, the invasive tracking and illicit surveillance technology that companies utilize to monitor consumers' movements across websites and throughout physical spaces would likely be viewed as a search if performed by government entities.[195]

---

[190] *See* Wayne Unger, *Katz and COVID-19: How a Pandemic Changed the Reasonable Expectation of Privacy*, 12 HASTINGS SCI. & TECH. L.J. 40, 62 (2020) [hereinafter *Katz & COVID-19*].

[191] *See id.* at 58.

[192] *Id.* at 62.

[193] *See* United States v. Jones, 132 U.S. 945, 955–58 (2012).

[194] *See id.* at 946–47.

[195] *Cf.* Andrew Guthrie Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47 (2020) (defining Professors David Gray and Danielle Citron's "technology-centered approach" to determining which types of surveillance technology constitutes a search for Fourth Amendment purposes as "any surveillance technology [that] 'has the capacity to facilitate broad programs of indiscriminate surveillance that raise the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of government'" in discussing the scope of Fourth Amendment protection in the context of "smart cities").

[57] In *Jones*, Justice Sotomayor's dissent contemplated the mosaic theory of privacy where individuals have a reasonable expectation that their movements will not be recorded and aggregated "in the sum" to infer one's personal beliefs, habits, and potentially sensitive information.[196] This form of data aggregation is exactly what occurs in the private sector when data brokers buy and sell consumers' personal information to amass detailed profiles of their lives.[197]

[58] The reasoning behind *Katz* and *Jones* is echoed throughout current privacy law proposals, though their holdings only apply to the government, leaving individuals vulnerable to exploitation from private entities.[198] After all, "the [g]overnment is no longer the primary infringer of privacy and security rights that individuals need protection from—private businesses are more powerful and intrusive than they have ever been before."[199]

2. Sectoral Laws

[59] The United States regulates privacy by providing individual protection to consumers who engage with specific industries such as the financial, credit, educational, video, and medical arenas.[200] The standards

[196] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 328 (2012).

[197] *See What Are Data* Brokers, *supra* note 1 (explaining that data brokers categorize consumers as subjects and assign them to various marketing categories).

[198] *See Katz & COVID-19*, *supra* note 190, at 61.

[199] Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH., no. 1, 2020, at 34 [*Reclaiming Our Right*].

[200] *See, e.g.*, Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended at 15 U.S.C. §§ 6801–6809 (2021)) (financial industry); Fair and Accurate Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended at 15 U.S.C. § 1681 (2021)) (credit business); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232(g) (2021) (education); Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified as amended at 18 U.S.C. § 2710 (2021)) (video industry).

and enforcement vary greatly by the industry. For example, the Gramm-Leach-Bliley Act provides protections for an individual's financial records,[201] the Fair and Accurate Transactions Act provides protections for an individual's credit report information,[202] the Family Educational Rights and Privacy Act provides protection for educational records,[203] the Video Privacy Protection Act prohibits "wrongful disclosure of video tape rental or sale records,"[204] and HIPAA provides protections for an individual's personal medical information.[205]

3. Private Tort Claims

[60] Modern privacy tort claims can be traced to Brandeis' and Warren's 1890 law review article.[206] Thanks to this scholarship, most states began to recognize invasion of privacy torts during the twentieth century.[207]

[61] Although the details of privacy tort claims are beyond the scope of this article, it is important to recognize that each privacy tort applies to a limited scope of harm. The four invasion of privacy torts recognized today are appropriation, intrusion on seclusion, public disclosure of private facts, and false light.[208] Appropriation occurs when the defendant utilizes the

[201] Gramm-Leach-Bliley Act §§ 6801–6809.

[202] Fair and Accurate Transactions Act § 1681.

[203] Family Educational Rights and Privacy Act § 1232.

[204] Video Privacy Protection Act § 2710.

[205] CONG. RSCH. SERV., LSB10490, HIPAA, TELEHEALTH, AND COVID-19 (2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10490 [https://perma.cc/W4Q6-TL2Q].

[206] *See* Warren & Brandeis, *supra* note 82, at 213–15, 219; *see also* WEAVER ET AL., *supra* note 83, at 285.

[207] *See* WEAVER ET AL., *supra* note 83, at 285.

[208] *Id.*

plaintiff's name or identity for commercial purposes.[209] Intrusion on seclusion occurs when the defendant intrudes upon the plaintiff's solitude or seclusion.[210] Public disclosure of private facts occurs when the defendant discloses private facts regarding the plaintiff "in a way that would be highly offensive and objectionable to a reasonable person of ordinary sensibilities."[211] False light occurs when the defendant casts the plaintiff in "a way that would be highly offensive to a reasonable person, and in reckless disregard for the truth or falsity of the publicized matter."[212]

[62] While privacy tort claims allow consumers some remedy for privacy harms, the litigation process can be time consuming and costly.[213] A federal privacy law would provide regulation and protection for all consumers, not only those with significant resources.

4. FTC Enforcement

[63] The FTC has the authority to prevent "unfair or deceptive acts or practices in or affecting commerce,"[214] which include actions that cause or are likely to cause significant injury to consumers in the privacy arena and beyond.[215] The FTC currently sanctions companies for unfair or deceptive

[209] *Id.* at 286.

[210] *Id.* at 288.

[211] *Id.* at 290.

[212] WEAVER ET AL., *supra* note 83, at 293.

[213] *See* Joe Palazzolo, *We Won't See You in Court: The Era of Tort Lawsuits Is Waning*, WALL ST. J. (July 24, 2017, 5:09 PM), https://www.wsj.com/articles/we-wont-see-you-in-court-the-era-of-tort-lawsuits-is-waning-1500930572 [https://perma.cc/56CW-UNTC] (noting that filing a tort lawsuit is "expensive and time-consuming").

[214] Goodyear, *supra* 77, at 82; 15 U.S.C. § 45(a)(1).

[215] *See* Scott Stiefel, *The Chatbot Will See You Now: Protecting Mental Health Confidentiality in Software Applications*, 20 COLUM. SCI. & TECH. L. REV. 333, 386 (2019).

practices while enforcing a company's adherence to its privacy policy.[216] Thus, the FTC can "only bring an enforcement action if a business manages consumer data in a way that runs contrary to its own privacy policy, violates existing federal privacy laws, or seriously injures consumers."[217]

5. State Privacy Laws

[64] Absent comprehensive federal privacy regulation, states have begun to pass their own privacy laws. While multiple bills have been introduced over the years, very few have been enacted into law.

[65] In 2008, Illinois became one of the first states to pass its own, narrow privacy law with the Biometric Information Privacy Act (BIPA).[218] BIPA regulates the collection and storage of biometric information, such as facial geometry and fingerprints, and requires biometric identifiers to be destroyed in a timely manner.[219] BIPA also provides for a private right of action[220] that has since generated several class actions.[221] In 2010, Massachusetts enacted the Standards for Protection of Personal Information of Residents of the Commonwealth that regulated the licensing and ownership of

[216] Nicole Angelica, *Alexa's Artificial Intelligence Paves the Way for Big Tech's Entrance into the Health Care Industry – The Benefits to Efficiency and Support of the Patent-Centric System Outweigh the Impact on Privacy*, 21 N.C. J.L. & TECH. 59, 77–78 (2020); *see also* discussion *supra* Section V.D.

[217] Jeevanjee, *supra* note 37, at 130; *see also Privacy and Security Enforcement*, *supra* note 99.

[218] *See generally* 740 ILL. COMP. STAT. ANN. 14/1 (2008) (actual text of BIPA).

[219] *See id.* at 14/15.

[220] *See id*. at 14/20.

[221] *See* Kimberly Gold et al., *Biometric Privacy: The year in review and looking toward 2020*, REED SMITH LLP: TECH. L. DISPATCH (Jan. 9, 2020), https://www.technologylawdispatch.com/2020/01/privacy-data-protection/biometric-privacy-the-year-in-review-and-looking-toward-2020/ [https://perma.cc/6A3G-WS6Z].

personally identifiable information of Massachusetts residents.[222] New York followed in 2017 by regulating the internet practices of financial institutions with the Cybersecurity Requirements for Financial Services Companies.[223]

[66] In 2014, the EU passed the broadly-encompassing European General Data Protection Regulation (GDPR), a law that applies to public and private businesses that meet two low establishment and targeting criterion thresholds.[224] The GDPR distinguishes itself as a pro-consumer format since it requires that consumers affirmatively opt in to the sharing and tracking of their personal identifying information[225] and provides a private right of action.[226] Though the GDPR is not a domestic law, it provides a successful framework for legislators to draw from when drafting privacy law.

[67] In 2018, the California Legislature agreed to pass the CCPA as a sort of concession to avoid a potentially stricter pending voter initiative.[227] The CCPA has fairly high thresholds, meaning it applies to larger businesses, provides consumers with the opt-out consent model, and only allows for a private right of action in certain circumstances.[228] In 2021, Virginia's Legislature became the first state to pass a comprehensive state

[222] *See* 201 MASS. CODE REGS § 17.01 (2010).

[223] *See* N.Y. COMP. CODES R. & REGS. tit 23, § 500.00 (2020).

[224] *See* GDPR, *supra* note 153, art. 3 (defining the "Territorial scope").

[225] *See id.* at art. 4(11) referenced in art. 6(1)(a) (defining opt-in consent).

[226] *See id.* at art. 79 (describing the private right of action).

[227] *See* Confessore, *supra* note 4.

[228] *See* discussion *infra* Section IV.B.

privacy law absent a pending voter initiative[229] with a pro-business model—the VCDPA—that only applies to certain large businesses.[230] The VCDPA uses an opt-out consent model and does not provide consumers with a private right of action.[231]

[68] In 2021, after much debate and revision, the Colorado Legislature passed the pro-business CPA, following Virginia's lead.[232] Like the VCDPA, the CPA applies to certain larger businesses, uses an opt-out consent model, and does not provide consumers with a private right of action.[233]

IV. THE REACH AND LIMITS OF THE GDPR, CCPA, VCDPA, AND CPA

[69] State-level privacy laws make the tangled web of regulation more complex. Each state privacy law includes its own definitions and requirements for various aspects of consumer privacy. This section provides a basic description of the GDPR and key state privacy laws, focusing on (1) to whom each law applies, (2) whether the opt-in or opt-out consent model is utilized, and (3) how the law is enforced. This analysis is important for informing the scope of a federal privacy law.

[229] Sarah Rippy, *Virginia passes the Consumer Data Protection Act*, INT'L ASS'N OF PRIVACY PROFS. (Mar. 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/ [https://perma.cc/US2A-DPRX].

[230] *See infra* Section IV.C.

[231] *See id.*

[232] *See* i*nfra* Section IV.D.

[233] *See* CPA, *supra* note 188.

A. GDPR—2014

[70] The EU has been a leader in consumer privacy protection since the early stages of the internet.[234] The EU adopted the European Data Protection Directive in 1995.[235] The directive was based on the privacy principle of notice, which refers to requirements that businesses only utilize consumer data for its designated purpose, and the prohibition against transferring consumers' information absent their consent.[236] In response to a growing movement advocating for online privacy rights, the European Parliament passed the GDPR in 2014 with a majority 621 out of 653 possible votes.[237]

[71] The GDPR, with its high level of consumer protection, falls on the strong end of the Privacy Spectrum. It applies to all entities located inside the EU as well as entities that target or "sell" the personal information of consumers in the EU.[238] It utilizes the opt-in consent model,[239] delegates enforcement to the Data Protection Authority (DPA), and provides for a private right of action under certain circumstances.[240]

---

[234] *See The History of the General Data Protection Regulation*, EUROPEAN DATA PROT. SUPERVISOR https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/H2FX-23XD] [hereinafter *History of GDPR*].

[235] *See id.*

[236] *See* Nate Lord, *What is the Data Protection Directive? The Predecessor to the GDPR*, DIG. GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [https://perma.cc/7W9V-Y3TR].

[237] *See History of GDPR*, *supra* note 234.

[238] *See* GDPR, *supra* note 153 (defining the Territorial Scope in Article 3).

[239] *See id.* (defining opt-in consent in Article 4(11), referenced in Article 6(1)(a)).

[240] *See id.* (describing the DPA's authority and data subjects' Private Right of Action in Articles 51 and 79).

[72] The GDPR applies to all entities categorized as data controllers or processors that process EU data subjects' personal data in connection with the offering of goods or services in the EU, or the monitoring of a subject's behavior occurring within the EU.[241] Unlike the CCPA, VCDPA, and CPA, the GDPR does not determine applicability based on narrow requirements of business revenue or consumer volume constraints.[242] This difference means that the GDPR conceivably applies to all public or private entities that "sell" consumers' personal information who are located in the EU.[243] The GDPR is unique because it applies to consumers who may not be EU residents but are located in the EU at the time of data collection.[244]

[73] The GDPR defines the sort of tracking and sharing of consumer personal information that requires opt-in consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[245] Recital 32 confirms that "[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent," and proscribes the business from burying a consent option inside lengthy legal agreements.[246]

[241] *See id.* (defining the Territorial Scope in Article 3).

[242] *See* Jennifer Lund, *WHAT IS GDPR AND HOW DOES IT IMPACT YOUR BUSINESS?* SUPEROFFICE (May 4, 2021), https://www.superoffice.com/blog/gdpr/ [https://perma.cc/5P6G-64PS] (discussing the broad applicability of the GDPR).

[243] *See* GDPR, *supra* note 153 (defining the Territorial Scope in Article 3).

[244] *See id.*

[245] *Id.* (defining "consent" at Article 4(11)).

[246] *Id.* (describing examples of practices that do not constitute consent).

[74] The GDPR is enforced under two modes: (1) a private right of action[247] and (2) through a DPA established in each member state.[248] The GDPR's private right of action allows data subjects the ability to seek redress for privacy violations in the national courts of member states when damages are caused by a data controller or data processor's breach.[249] DPAs have the authority to interpret the GDPR with significant auditing and investigative powers.[250] The GDPR preempts individual privacy laws in member states and applies to both public and private parties.[251] Thus, the GDPR is enforced in the EU through both government enforcement (the DPAs) and a private right of action.[252] While the United States currently lacks a federal private right of action, this article proposes that privacy enforcement should function the same way as it does under the GDPR.

B. CCPA—2018

[75] Enacted in 2018, the CCPA provided consumers some privacy rights.[253] The CCPA was further expanded by the CPRA, approved as a California ballot proposition by a majority of voters in the November 2020 general election.[254] The CCPA is close to the middle ground of the Privacy

[247] *Id.* (defining the Private Right of Action at Article 79).

[248] *See* GDPR, *supra* note 153 (describing the DPA for each member state and the rules that apply at Article 51).

[249] *Id.* (defining the Private Right of Action at Article 79).

[250] *Id.* (defining the DPA authority at Articles 51 and 58).

[251] *Id.* (defining the Material and Territorial Scope at Articles 2 and 3); *see also EU General Data Protection Regulation*, ELEC. PRIV. INFO. CTR., https://epic.org/international/gdpr/ [https://perma.cc/8PFW-TYJ2].

[252] GDPR, *supra* note 153 (describing the DPA authority and data subjects' Privacy Right of Action at Articles 51 and 79).

[253] Cal. Civ. Code § 1798.100 (Deering 2021).

[254] *CPRA Executive Summary*, *supra* note 128.

Spectrum, providing some protection to consumers, yet still allowing some harm. The CCPA only applies to businesses that meet certain volume or revenue thresholds, is based on an opt-out consent model, and is enforced by the California attorney general and the California Privacy Protection Agency.[255] Additionally, the CCPA provides consumers with a private right of action under certain circumstances.[256]

[76] The CCPA only applies to California residents and is only enforceable against companies that (1) derive over 50% of their revenue from selling consumers' information, (2) have an annual gross revenue exceeding $25 million, or (3) interact in a specified format with over 50,000 personal accounts.[257] This narrow threshold leaves smaller businesses and other entities who sell a significant volume of personal information untouched. In complying with the CCPA, many companies extend their CCPA-compliant policies nationwide for simplicity's sake.[258]

[77] The CCPA defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[259]

[78] The sweeping definition of a "sale" of one's data applies to "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other

[255] Cal. Civ. Code §§ 1798.100, 120, 140, 155 (Deering 2020).

[256] Goodyear, *supra* note 77, at 83–84.

[257] Cal. Civ. Code §§ 1798.140(c)(1) (Deering 2021).

[258] Michael Williams, *IAB Finds That Businesses Are Adopting CCPA Protocols Nationwide – But Should They?* CLYM (Nov. 22, 2020), https://www.clym.io/iab-finds-that-businesses-are-adopting-ccpa-protocols-nationwide-but-should-they/ [https://perma.cc/2N9Y-FVQD].

[259] Cal. Civ. Code § 1798.140(o) (Deering 2021).

means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[260]

[79] The opt-out consent model requires businesses to comply with a consumer's request to opt out of the sale of their personal information to third parties, subject to certain exceptions.[261] Businesses are required to include a "Do Not Sell My Personal Information" link on a website's homepage in a clear and conspicuous location.[262]

[80] In response to "website designs that can confuse or trick users into opting into selling their information," the CCPA was amended to include the Dark Patterns law in 2021.[263] This law further enforces the link requirement and prevents businesses from making the process too lengthy, confusing, or onerous for consumers.[264]

[81] A service provider is defined as a legal entity organized for profit that "processes [personal] information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity . . . from retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."[265] The private right of action available for

[260] *Id.* § 1798.140(t)(1).

[261] *Id.* §§ 1798.120, 1798.135(a)–(b).

[262] *Id.* § 1798.135(a)(1).

[263] Allana Akhtar, *California is banning companies from using 'dark patterns,' a sneaky website design that makes things like canceling a subscription frustratingly difficult*, BUS. INSIDER (Mar. 16, 2021, 12:32 PM), https://www.businessinsider.com/what-are-dark-patterns-2021-3 [https://perma.cc/3S3J-Z5UZ].

[264] *See id.*

[265] Cal. Civ. Code § 1798.140(v) (Deering 2021).

certain data breaches involves a narrow set of personal information.[266] Consumers are allowed to seek the greater of statutory damages ranging from $100 to $750 per consumer per incident or actual damages.[267] Additionally, courts are allowed to impose declaratory or injunctive relief.[268]

C. VCDPA—2021

[82] In 2021, Virginia passed the VCDPA.[269] Due to the lack of federal privacy legislation and the growing concern of constituents, the VCDPA was rushed through in one session without sufficient time for debate and testimony.[270] The text of the VCDPA was originally presented to State Senator David Marsden by an Amazon lobbyist.[271] Senator Marsden pushed the law through the legislature.[272] The VCDPA is on the weak end of the Privacy Spectrum, providing low protection with a high risk of harm to consumers. The VCDPA only applies to a narrow scope of businesses, relies on the opt-out consent model, does not provide a private right of action to

[266] *Id.* § 1798.150(a)(1).

[267] *Id.* § 1798.150(a)(1)(A).

[268] *Id.* § 1798.150(a)(1)(B).

[269] *See* S.B. 1392, 2021 Gen. Assemb., Reg. Sess. (Va. 2021).

[270] *Consumer and Privacy Groups Urge Virginia Governor to Veto or Send Privacy Bill Back to Legislature*, CONSUMER FED'N AM. (Feb. 25, 2021), https://consumerfed.org/press_release/consumer-and-privacy-groups-urge-virginia-governor-to-veto-or-send-privacy-bill-back-to-legislature [https://perma.cc/B3KX-DMRP] (statement of Director Susan Grant) ("Consumer representatives were not given a fair hearing as this bill was rushed through the legislative process.").

[271] *See* Tsukayama, *supra* note 160 (explaining that VCDPA was introduced to the bill's sponsor by an Amazon lobbyist); S.B. 1392 (indicating State Senator David Marsden as the bill's sponsor).

[272] *Id.*

consumers, and relies solely on Virginia's attorney general for enforcement.[273]

[83] The VCDPA applies to entities that "conduct business in the Commonwealth or produce products or services that are targeted to residents of the Commonwealth and that (i) . . . control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."[274] Because there is no revenue threshold, the VCDPA does not apply to smaller businesses unless they fall under one of the two categories.[275]

[84] The VCDPA only applies to sales of data that are based on monetary consideration.[276] This contrasts with the CCPA, which extends the definition of a sale to when personal data is exchanged for either monetary or other valuable consideration.[277] Limiting the scope of a 'sale' gives businesses free range to work out quid pro quo deals to share consumers' information absent monetary exchanges. For example, Facebook's information sharing deals with 150 other businesses would likely be exempt from VCDPA enforcement if no actual money was exchanged.[278] Thus,

[273] *See* S.B. 1392, 2021 Gen. Assemb., Reg. Sess. (Va. 2021).

[274] *Id.* § 59.1-572(A) (defining the scope of the VCDPA).

[275] *Id.*

[276] *Id.* § 59.1-571 (defining the "sale of personal data").

[277] *See* Cal. Civ. Code § 1798.100(t) (Deering 2021).

[278] *See e.g.*, Nicholas Confessore et al., *Facebook offered users privacy wall, then let tech giants around it*, SEATTLE TIMES, (Jan. 14, 2019, 12:09 PM), https://www.seattletimes.com/business/facebook-offered-users-privacy-wall-then-let-tech-giants-around-it/ [https://perma.cc/9DS8-LLEZ] (detailing the special arrangements where "Facebook gave some of the world's largest technology companies more intrusive access to users' personal data than it has disclosed"); *see also infra* Section VI.A (describing Facebook's claims that it is a service provider).

such enormous disclosures of consumers' personal information would not be subject to the VCDPA.

[85] The VCDPA specifically exempts disclosures to business' affiliates from regulation.[279] Thus, any business that meets the narrow requirements of the VCDPA to begin with is still free to share consumers' personal information with a wide range of other entities if they categorize them as affiliates.

[86] The pro-business opt-out model provides consumers the right to opt out of the processing of their personal data for targeted advertising purposes, profiling, and the sale of their personal data.[280] Unlike the CCPA, the VCDPA provides a narrow exception for certain sensitive personal information absent consumer consent.[281] While this small exception is a step toward consumer privacy, the opt-out model still applies to a significant portion of data processed.

[87] Additionally, the VCDPA's lack of a private right of action means that enforcement is left to the discretion of Virginia's attorney general.[282]

D. CPA—2021

[88] In 2021, after amendments from the State Senate and the House, the Colorado Legislature passed the CPA.[283] The CPA joined the recently

[279] *See* S.B. 1392, 2021 Gen. Assemb., Reg. Sess., § 59.1-571 (Va. 2021) (describing how a sale of personal data does not include data transferred to an affiliate).

[280] *See id.* at § 59.1-573 (describing the opt-out consent model).

[281] *See id.* at § 59.1-574 (requiring data controllers to obtain consumers' consent prior to processing sensitive data).

[282] *See id.* at § 59.1-580 (describing how the Virginia Attorney General has exclusive authority to enforce the VCDPA).

[283] *See generally* CPA, *supra* note 188 (The General Assembly of the State of Colorado signed the Colorado Privacy Act on June 25, 2021.).

enacted VCDPA on the weak end of the Privacy Spectrum providing low consumer protection and a high risk of harm. The House instituted volume and revenue thresholds to only implicate larger businesses, sided with the pro-business opt-out consent model, and eliminated the private right of action.[284]

[89] The CPA included seemingly pro-consumer statements like "Colorado will be among the states that empower consumers to protect their privacy and require companies to be responsible custodians of data as they continue to innovate," and, "the unauthorized disclosure of personal information and loss of privacy can have devastating impacts ranging from financial fraud, identity theft, and unnecessary costs in personal time and finances to destruction of property, harassment, reputational damage, emotional distress, and physical harm."[285] Statements like this may lead the reader to believe this bill will provide adequate protection for consumers, but it is important to note that the legislature removed strong consumer protection features.[286]

[90] The CPA only applies to an entity that "conduct[s] business . . . or produces . . . products or services that are intentionally targeted to residents of Colorado; and . . . (I) controls or processes the personal data of [100,000] consumers or more during a calendar year; or (II) derives revenue . . . from the sale of personal data and . . . processes or controls the personal data of [25,000] consumers or more," with exceptions for personal data governed by other laws.[287] By including the qualifier that products or services must

[284] *See id.* at §§ 6-1-1304, 6-1-1306, 6-1-1311.

[285] *Id.* at § 6-1-1302.

[286] *See* Stauss et al., *supra* note 186 (discussing how the Senate's amendments required the pro-consumer elements of opt-in consent and a private right of action and that these pro-consumer amendments that would have supported the above language were reversed by the House right before the bill passed).

[287] CPA, *supra* note 188, at § 6-1-1304.

be "intentionally targeted to residents of Colorado,"[288] one could suspect businesses will use this as a loophole. For example, a business could claim it did not intentionally target anyone and the Colorado residents found the business independently through an internet search engine.

[91] The CPA provides consumers with rights to opt out of the collection, processing, and sale of their personal data.[289] As noted by privacy advocates, this consent model typically only affects those consumers that care the most about their privacy and have the time, sophistication, and education to go through the sometimes onerous process of opting out.[290] The CPA does include a narrow opt-in consent model for "sensitive" personal data, which applies to data regarding religious beliefs, sexual orientation, race/ethnicity, citizenship status and physical or mental health information.[291]

[92] The Colorado Legislature removed the private right of action from the CPA, so enforcement now falls solely on the Colorado attorney general or district attorneys.[292] Without a private right of action as personal redress, individual consumers must rely on government entities to initiate an investigation, which often will not occur until there are multiple reports of violations.[293]

[93] The next section will expand on the individual laws and their correlation to the components included in this article's proposal.

[288] *Id.*

[289] *See id.* at § 6-1-1306.

[290] *See* Hindi, *supra* note 47.

[291] *See* CPA, *supra* note 188, at §§ 6-1-1303, 6-1-1308.

[292] *See id.* at § 6-1-1311.

[293] *See Reclaiming Our Right*, *supra* note 199, at 13–14.

V. CRUCIAL ELEMENTS NECESSARY FOR FEDERAL PRIVACY LEGISLATION

[94] The United States has fallen behind other countries that are passing legislation to protect their consumers' data.[294] United States privacy law "does not reflect the reality that the internet and connected services and devices have been integrated into every facet of our society."[295] Research has shown that a majority of Americans do not believe their personal data is secure and strongly favor more government privacy regulation.[296] Thus, the iOS 14.5 update data should come as no surprise.

[95] Under the current landscape, "[s]ome of privacy law's most important tools—including privacy by design, consent requirements, and FTC consent decrees—are so unclear that professionals on the ground have wide latitude to frame the law's requirements."[297] According to Ari Waldman, a Professor of Law and Computer Science at Northeastern University School of Law, "consumers more often than not lose out" when businesses are left to interpret ambiguous privacy laws, while focusing on corporate profits.[298]

---

[294] *See* Jeevanjee, *supra* note 37, at 130.

[295] *Examining Legislative Proposals to Protect Consumer Data Privacy: Hearing Before the S. Comm. on Commerce, Sci., & Tech.*, 116th Cong. (2019) (statement of Michelle Richardson, Director, Privacy and Data Center for Democracy and Technology); Jeevanjee, *supra* note 37, at 130.

[296] *See* BROOKE AUXIER ET AL., PEW RSCH. CTR, AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 1, 4, 6, 28, 43 (Nov. 15, 2019) (noting that 81% of American adults do not feel they have control over the data collected by companies about them and 81% of American adults believe the "[p]otential risks of . . . companies . . . collecting data about them outweigh[s] the benefits").

[297] Waldman, *supra* note 38, at 777.

[298] *See id.*

[96] This section will discuss why federal privacy law should (1) apply to all entities that sell consumer information, (2) require consumers' affirmative opt-in consent, (3) include a private right of action, (4) be enforced by the FTC, and (5) include federal preemption. This section concludes with a short summary of why federal privacy law should not be modeled after the VCDPA and CPA.

A. Privacy Regulation Should Apply to all Entities Selling Consumer Information

[97] Federal privacy regulation should draw from the GDPR's broad scope of categorization[299] and apply to all entities that sell[300] a consumer's personal information for valuable consideration. The CCPA, VCDPA, and CPA only apply to a narrow subset of businesses based on sales volume or revenue. This leaves some larger players and most small businesses unregulated. The GDPR, however, applies to a broader range of entities that process EU data subjects' personal data in connection with monitoring their behavior or offering goods or services in the EU.[301] As there is no required revenue or volume threshold, the GDPR, which applies to all entities that sell a user's personal information when located in the EU, provides broader consumer protection.[302]

[98] The risk to consumers from sharing their personal information[303] is the same whether it comes from a mammoth online retailer like Amazon, a small start-up based in a garage, or brick and mortar retail stores. The segregation of companies into classes is discriminatory in nature because it

[299] *See* discussion *supra* Section IV.A.

[300] *See* Cal. Civ. Code § 1798.140(t) (Deering 2021) (defining the sale of information under the CCPA).

[301] *See* GDPR, *supra* note 153 (defining the Territorial Scope in Article 3).

[302] *See id.*

[303] S*ee* discussion *supra* Section II.

allows most small businesses and some larger entities to evade regulation if they sell consumers' personal information.[304] This classification has the same effect as allowing a business to engage in unfair or deceptive practices, so long as it does not earn a certain amount of revenue while doing so. If society values privacy, as has been shown by the roots of the FIPPs in 1973, the Privacy Act in 1974,[305] and the results of the iOS 14.5 update in 2021,[306] the original concept of notice and consent should be the floor, not the ceiling, for doing business in the United States.

[99] Big Tech favors privacy regulation that applies to all businesses that collect and sell consumers' personal information, including retail brick and mortar stores.[307] Big Tech also argues that state privacy regulation is specifically targeted to hinder large technology companies, as opposed to small businesses that engage in the same practices.

[100] Some critics argue that privacy laws should only apply to large tech firms with significant resources. For example, some privacy professionals argue that privacy legislation should "exclude businesses with limited financial and/or personnel resources, i.e. small businesses."[308] This belief stems from the potential disadvantages small businesses may encounter when faced with compliance costs in the marketplace.[309] However, privacy compliance is now a necessary expenditure that should be built into every business plan from the start. If a business model respects consumer privacy

[304] *See, e.g.*, GDPR, *supra* note 153 (applying to all entities that sell consumer private information).

[305] *See* discussion *supra* Section III.A.1 (describing the FIPPs and The Privacy Act of 1974).

[306] *See* discussion *infra* Section V.B.2 (describing the iOS 14.5 update results).

[307] *See* Berroya, *supra* note 54.

[308] Diane Y. Byun, *Privacy or Protection: The Catch-22 of the CCPA*, 32 LOY. CONSUMER L. REV. 246, 246 (2020).

[309] *Id.* at 249–50.

and does not sell personal information without consent, there would be minimal, if any, additional expenses.[310]

[101] By placing volume or revenue thresholds on the applicability of privacy laws, as the CCPA, VCDPA, and CPA do, unscrupulous entities may attempt to evade the law. A company could branch off into multiple smaller companies to stay under the threshold limits and continue selling consumers' data while evading the reach of regulators. With advanced technology, systems can be programmed to automatically collect and share consumers' information every time they visit a website, or when information is entered into a business's database.[311]

[102] The United States should follow the GDPR's lead to apply federal privacy law to all businesses—regardless of volume or revenue—that sell data related to consumers located in the United States.

B. The Opt-In Consent Model is Necessary

[103] In 2000, the FTC called on Congress to pass legislation requiring every online business to provide consumers with the choice of how their data is used beyond the original purpose for which it was provided.[312] This affirmative opt-in consent model was echoed in 2012 with the Obama administration's CPBR and has been a focal point of privacy advocates for decades.[313]

---

[310] *See* Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1373, 1440, 1442 (2017) (explaining that companies can use various PFP schemes to counter the expenses to protect and/or use consumer data).

[311] *See* Emily Stewart, *How big business exploits small business*, VOX (Jun. 30, 2021, 8:00 AM), https://www.vox.com/the-goods/22550608/how-big-business-exploits-small-business [https://perma.cc/67GU-VSYU]; Alexander S. Gillis, *What is internet of things (IoT)?*, TECHTARGET, https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT [https://perma.cc/WLA3-R7VB].

[312] *See* Rich, *supra* note 40.

[313] *See supra* Section III.A.3 (providing a brief history of the CPBR).

[104] Professor Joseph Tomain[314] argues that "the law has lost sight of the interests of individual human beings in the online data processing context because there has been an overemphasis on the rights and freedoms of data processors and an undervaluing of the rights and freedoms of individuals."[315] According to Tomain, the opt-out consent model is ineffective because individuals frequently fail to exercise their privacy rights, the scope available to opt out may be limited, and the processes required may be difficult.[316] Tomain supports the opt-in consent model as "an important part of the solution to the new privacy challenges arising in the Big Data era because it helps us regain sight that law operates first and last, for, upon, and through individual human beings."[317]

[105] The International Association of Privacy Professionals (IAPP) is an organization that markets training and certifications to data privacy professionals in Asia, Canada, Europe, and the United States.[318] Many privacy-related jobs now require IAPP designations.[319] In February 2019, IAPP published an article for their privacy professional members describing how opt-in consent works.[320] The article explained IAPP's positions

[314] *See Joseph A. Tomain*, IND. UNIV. BLOOMINGTON, https://law.indiana.edu/about/people/bio.php?name=tomain-joseph [https://perma.cc/8KWH-CHX6] (explaining that Professor Joseph A. Tomain teaches Privacy Law and Internet Law at the Maurer School of Law).

[315] Joseph A. Tomain, *Online Privacy & the First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV., 1, 70 (2014).

[316] *See id.* at 24–26.

[317] *See id.* at 71.

[318] *See CIPP Certification*, INT'L ASS'N OF PRIVACY PROFS., https://iapp.org/certify/cipp/ [https://perma.cc/R88J-HUPC].

[319] *See Certified Information Privacy Cipp Jobs*, INDEED, https://www.indeed.com/q-Certified-Information-Privacy-Cipp-jobs.html [https://perma.cc/9CP9-SRAU].

[320] *See* Rita Heimes, *How opt-in consent really works*, INT'L ASS'N PRIV. PROFS. (Feb. 22, 2019), https://iapp.org/news/a/yes-how-opt-in-consent-really-works/ [https://perma.cc/ES7T-47UD].

regarding email marketing and cookies.[321] According to Phil Lee, partner at the Fieldfisher law firm in London, "the regulatory view these days is that consent has to be opt-in to meet the requirement that consent be 'affirmative' – and you have to get that consent before any cookies (excepting strictly necessary cookies) are dropped."[322] "IAPP took a very conservative — that is to say, very privacy-friendly — view of cookie consent, putting all marketing and analytics cookies in the 'non-essential' category and setting them not to drop until a visitor agrees (opts in) to receive them."[323]

[106] The Individual Control prong of the CPBR recognized the need for simplicity in obtaining consent.[324] This prong expounds that "consumers have a right to exercise control over what personal data companies collect from them and how they use it . . . Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place."[325] Absent federal regulation in the past decade, businesses resorted to doing the exact opposite of this prong's intent.

---

[321] *See id.*; *see also* Dave Johnson, *A guide to internet cookies, the small files that store information about your online activity*, BUS. INSIDER (Apr. 6, 2021, 9:50 AM), https://www.businessinsider.com/what-are-cookies?r=US&IR=T [https://perma.cc/5QPS-J63R] (explaining that a cookie is a small text file stored on your computer by websites with the purpose of cookies ranging from those required for a website to function to tracking cookies utilized by third parties and that third-party cookies can be used to "track your online activities across the internet, like the pages you've visited and products you've looked at").

[322] *See* Heimes, *supra* note 320.

[323] *See id.*

[324] *See* WHITE HOUSE PRIVACY REPORT, *supra* note 13, at 11.

[325] *See id.*

[107] Until the GDPR and CCPA took effect, consumers were not notified by the majority of websites that their personal information was being collected, stored, and shared with third parties. Many websites that fall under the GDPR and CCPA's regulation have buried this choice in legally complex notices that most consumers never read.[326] As the CCPA utilizes an opt-out consent model, businesses are allowed to continue tracking and sharing the personal information of consumers that do not complete the extra task of opting out.[327] Thus, federal privacy law needs to require a clear and simple opt-in consent model that presents consumers with the ability to affirmatively control whether their personal data is tracked or sold.

[108] An excellent example of the format for opt-in consent was found in an early version of the CPA that ultimately did not pass.[328] The CPA's early definition of consent below illustrated the opt-in model by clearly articulating not only what consent meant, but also by providing examples of what it did not include. The revised Senate bill defined consent as:

> "[a] clear, affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement, such as a written statement, including by electronic means or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Consent does not include (a) 'acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information'; (b) 'hovering over, muting,

[326] *See* Caitlin Chin, *Highlights: The GDPR and CCPA as benchmarks for federal privacy legislation*, BROOKINGS INST. (Dec. 19, 2019), https://www.brookings.edu/blog/techtank/2019/12/19/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/ [https://perma.cc/ZK9D-D5MU]; *see* Hindi, *supra* note 47.

[327] *See* Cal. Civ. Code § 1798, 120, 135(a)–(b) (Deering 2021).

[328] *See* Stauss et al., *supra* note 186.

> pausing, or closing a given piece of content'; and (c) 'agreement obtained through dark patterns.'"[329]

[109] Dark patterns are defined as "[a] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice." [330] In the last week of its 2021 session, the Colorado Legislature amended the bill to only provide consumers with an opt-out consent model.[331]

[110] Under the CCPA, the opt-out model provides companies the ability to skirt around the law and make it difficult, and in some cases impossible, for a consumer to opt out.[332] These behaviors led to the Dark Patterns law that prohibits companies from making it difficult for consumers to opt out of information sharing.[333] The new law states that "[a] business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. *A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out.*"[334] While the intentions of the law to eliminate deceptive behavior were good, it is not clear enough as drafted; it still leaves room for companies to argue that their design is not intended to impair the consumer's choice and thus, it should not apply.

---

[329] *See id.*

[330] *See id.*

[331] *See id.*

[332] *See* Adam Nyhan, *New California Privacy Law Bars "Dark Patterns" That Hinder Opt-Outs*, PERKINS THOMPSON (Mar. 18, 2021), https://www.perkinsthompson.com/new-california-privacy-law-bars-dark-patterns-that-hinder-opt-outs/ [https://perma.cc/79S2-HDBE] (providing that on March 15, 2021, California's Attorney General announced its new Dark Patterns law).

[333] *See id.*

[334] *Id.* (emphasis added).

[111] Casey Fiesler, a data privacy and ethics fellow of the Silicon Flatirons Institute at the University of Colorado Law School, believes the opt-out model would likely only impact those individuals that really do care about their privacy as people often "accept terms of agreement without fully reading or understanding them."[335] Fiesler argues there is "'a big gap between the people who are really paying attention to this and really care about their privacy and are going to all of this extra work to protect their privacy,' . . . 'and the average person who's just like, "I want to go on Facebook, I want to go use Amazon, and, oh I have to click through a thing."'"[336] Thus, privacy proponents support the opt-in consent model where the consumer's personal information remains private unless the consumer actually asks for the company to collect and share it.[337]

[112] An article published in the Loyola of Los Angeles Law Review argues for the opt-in consent model with a twist.[338] In addition to the increased privacy under the opt-in structure, the article describes a framework for providing "greater incentives for companies to pay consumers for their data."[339] While this is desirable from the consumer's perspective, it seems that Congress can still utilize the opt-in consent model to protect consumers without imposing additional costs on businesses.

[113] It is imperative the United States require a firm opt-in consent model. Without it, even a business that specializes in data privacy will resort to the way that best suits its marketing goals. For example, IAPP was a leader in providing true opt-in consent in 2019, even though the full cookie

[335] *See* Hindi, *supra* note 47.

[336] *Id.*

[337] *Id.*; *see also* Tsukayama, *supra* note 160.

[338] *See* Rebecca Harris, *Forging a Path Towards Meaningful Digital Privacy: Data Monetization and the CCPA*, 54 LOY. L.A. L. REV. 197 (2020).

[339] *Id.*

acceptance rate was only 34%.[340] In November 2020, IAPP reversed its privacy practices from utilizing opt-in consent for cookies everywhere, to only utilizing it in the EU and United Kingdom, as required by the GDPR.[341] IAPP disclosed that it was "maintaining the opt-in features for first-party analytics and marketing cookies for site visitors from the European Union and United Kingdom but [was] [] offering an opt-out experience for site visitors from all other regions."[342] Even a reputable privacy-concerned organization will resort to the minimum requirements necessary when given the opportunity. This privacy reversal provides further evidence the United States must base its federal privacy regulation around the opt-in consent standard, as featured in the iOS 14.5 update.

1. Privacy Policies are not a Substitute for Opt-In Consent

[114] Absent a comprehensive federal privacy law, many businesses operate under the assumption that the fine print of a legally complex privacy policy will sufficiently show good faith toward consumers. While the FTC does provide enforcement against a business that deviates from practices disclosed in its privacy policy,[343] privacy policies are often not a simple solution to provide consumers with notice and consent options. Many privacy policies utilize language designed to lead consumers to believe the company protects their information.[344] This often leads consumers to

[340] *See* Heimes, *supra* note 320 (explaining why IAPP was taking a very privacy friendly approach to cookies).

[341] *See* Rita Heimes, *Changes in IAPP's cookie tool*, INT'L ASS'N OF PRIVACY PROF'LS (Nov. 12, 2020), https://iapp.org/news/a/changes-in-iapps-cookie-tool/ [https://perma.cc/7SMT-YPG2].

[342] *Id.*

[343] *See* Angelica, *supra* note 216, at 77–78; *see also* discussion s*upra* Section V.D.

[344] *See* FORBRUKERRADET, DECEIVED BY DESIGN 22 (2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf [https://perma.cc/XY8J-VF75] (discussing how Big Tech utilizes positive and negative wording to "nudge users toward accepting data collection").

automatically click on 'accept' when they may not really understand what is occurring.[345] Businesses then profit off sharing data with third parties.[346]

[115] In 2012, the average length of an online privacy policy was 2,514 words.[347] It would take an average internet user seventy-six working days—consisting of eight hours per day—to read the privacy policies of every website they encountered within a year.[348] Despite advanced technology, the typical internet browser's current format is such that a consumer cannot review a company's privacy policy prior to entering their site.[349] Thus, under the opt-out consent model, consumers cannot opt out of the sharing of their information until they have already visited the website. This further reinforces why an affirmative opt-in consent prompt should appear prior to entering any website, just like an app is required to do on Apple's iOS 14.5 operating system.

2. The iOS 14.5 Update Supports Current Constituents' Preferences

[116] United States consumers' demand for privacy, as exemplified by the Apple iOS 14.5 update feedback, should be utilized by Congress when enacting comprehensive federal privacy law. When faced with a simple, easy to understand standalone screen that specifically asks the user if they want to be tracked, utilizing language such as "Allow 'App' to track your

[345] *See* Hindi, *supra* note 47.

[346] *See What Are Data* Brokers, *supra* note 1 (discussing the $200 billion dollar data broker industry).

[347] Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Day*s, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/9ZR5-WNWC].

[348] *Id.*

[349] *See* Heimes, *supra* note 320.

activity across other companies' apps and websites?",[350] 85% of iOS users in the United States said no.[351] iOS has the predominant market share—at 59%—in the United States for all mobile device operating systems.[352] This significant metric illustrates that when given a simple, understandable choice, consumers do not want their personal information to be shared.

[117] The iOS 14.5 update has been hailed as a "landmark update" due to its enhanced privacy features that reinforce Apple's commitment to protecting consumers by implementing an "App Tracking Transparency" policy for all apps on iOS devices with the update.[353] "The hallmark of the feature is that app providers will have to request permission from users before they can begin to track them on any third-party websites or apps."[354] As Apple CEO Tim Cook explained, "we see a world where if everybody thinks they're being tracked all the time, then that will result in people changing their behavior. [. . .] They'll begin to think less, they'll begin to search less, they'll begin to not express themselves fully. And that narrow world is not one that any of us should aspire to live in."[355]

[118] While this privacy step has been warmly received by privacy advocates, businesses that center on collecting and sharing consumer personal information have expressed concern.[356] For example, Google

[350] *See iOS Update*, *supra* note 34.

[351] *See* Laziuk, *supra* note 36.

[352] STATCOUNTER, *supra* note 32.

[353] Sumeet Wadhwani, *Apple's Soon-to-Be Rolled Out iOS 14.5 Puts Facebook in a Spin and Mark Zuckerberg Can Do Nothing About It*, TOOLBOX (Apr. 29, 2021) https://www.toolbox.com/tech/it-strategy/news/apples-soon-to-be-rolled-out-ios-14-5-puts-facebook-in-a-spin-and-mark-zuckerberg-can-do-nothing-about-it/ [https://perma.cc/KWD9-FNCX].

[354] *Id.*

[355] *Id.*

[356] *See id.*

determined that by disabling third-party cookies, its programmatic advertising based on tracking would decline the average publisher's revenue by 52%.[357] If Apple can implement privacy measures to protect consumers under a business model that generates $274 billion dollars in annual revenue,[358] other businesses should be able to comply with privacy requirements while remaining profitable.

[119] In response to the pending iOS 14.5 update, Facebook launched an ad campaign against Apple claiming the update could decrease 60% of small business sales.[359] An estimated 50% of Facebook's revenue is derived from personalizing ad content to individual consumers.[360] Apple delayed its originally scheduled implementation of the privacy opt-in feature to provide businesses, such as Facebook, time to prepare for it.[361]

[120] In June 2021, Facebook announced it will begin selling a smartwatch with two cameras, one of which focuses on the consumer when they check the time.[362] The smartwatch is "part of Facebook CEO Mark Zuckerberg's plan to build more consumer devices that circumvent Apple

[357] *Id.*

[358] *See* Vailshery, *supra* note 33.

[359] Dan Levy, *Speaking Up for Small Businesses*, META (June 30, 2021, 10:10 AM), https://about.fb.com/news/2020/12/speaking-up-for-small-businesses/ [https://perma.cc/L6NM-W5R6].

[360] Wadhwani, *supra* note 353.

[361] *See* Kif Leswing & Megan Graham, *Apple delays iPhone change that's expected to make it harder for Facebook and other apps to target ads*, CNBC (Sept. 3, 2020, 3:45 PM), https://www.cnbc.com/2020/09/03/apple-delays-privacy-focused-iphone-change-that-could-affect-facebook.html [https://perma.cc/S82Z-J4UM].

[362] *See* Alex Heath, *Facebook plans first smartwatch for next summer with two cameras, heart rate monitor*, VERGE (June 9, 2021 1:26 PM), https://www.theverge.com/2021/6/9/22526266/facebook-smartwatch-two-cameras-heart-rate-monitor [https://perma.cc/WD28-QPTA].

and Google, the two dominant mobile phone platform creators that largely control Facebook's ability to reach people."[363]

[121] After Apple released the iOS 14.5 update and the low opt-in rate was making the news, Google responded by announcing it would improve privacy. Google will begin providing Android mobile device users with the right to opt out of personalized tracking in late 2021.[364] Google agreed to implement the opt-out consent model,[365] which tends to have minimal impact on consumer data privacy as only a small segment of the population have the time, sophistication, or knowledge to participate.[366] Although this is one example of a company improving its privacy practices in the absence of federal privacy legislation, Google is far more the exception than the rule because it has exorbitant resources available to make product changes in response to competition.[367]

[122] Some critics may argue that due to the iOS update data, a federal law is not needed as companies will compete on their own over privacy. For example, Google responded to the iOS update by agreeing to provide Android users with the opportunity to opt out of data tracking.[368] While this move does not rise to the level of Apple's affirmative opt-in consent model, it does show that Google recognizes the privacy component of a competitive market. Facebook took the opposite approach by developing new hardware

[363] *Id.*

[364] Ravie Lakshmanan, *Google to Let Android Users Opt-Out to Stop Ads From Tracking Them*, HACKER NEWS (June 4, 2021), https://thehackernews.com/2021/06/google-to-let-android-users-opt-out-to.html [https://perma.cc/CHB2-MJNT].

[365] *See id.*

[366] *See* Hindi, *supra* note 47 (discussing how the opt-out consent model typically only applies to those consumers who understand and take time to endure the many processes).

[367] See ALPHABET, YEAR IN REVIEW 2020 (2020), https://abc.xyz/investor/static/pdf/2020_alphabet_annual_report.pdf?cache=8e972d2 [https://perma.cc/C74U-ZWQ2].

[368] *See* Lakshmanan, *supra* note 364.

devices of its own so that it may continue its data collection, absent restrictions from Apple or Google.[369]

[123] As previous examples have shown, absent federal regulation, businesses tend to resort to the minimum compliance necessary.[370] Therefore, this proposal argues that federal privacy legislation is necessary to ensure all businesses comply with the best consumer protection practices available.

[124] Additionally, it is important that regulators ask the right question at this critical time—do consumers want their personal habits to be tracked and their personal information to be shared?[371] With the explosive growth of Big Tech, the wrong questions are frequently asked, leading to time-consuming investigations and endless debate, while ignoring the key privacy issues.[372] For example, Google partnered with Ascension, the largest nonprofit health system in the United States, which allowed Google to access the medical records of fifty million people.[373] The key questions asked by regulators and journalists at the advent of this partnership related to compliance with health laws and consent. Regulators failed to focus on the future use and underlying purposes for this data.[374] According to Professor Mason Marks, an even bigger concern is what Google plans to do

[369] *See* Heath, *supra* note 362.

[370] *See* Heimes, *supra* note 341 (discussing IAPP's decision to reverse its cookie policy in favor of tracking outside of the GDPR, where it is required).

[371] *See generally* Mason Marks, *The Right Question to Ask About Google's Project Nightingale*, SLATE (Nov. 20, 2019, 10:47 AM), https://slate.com/technology/2019/11/google-ascension-project-nightingale-emergent-medical-data.html [https://perma.cc/Q4JJ-ZA2P] (explaining how regulators asked Google questions about its Project Nightingale that took the focus away from consumer privacy issues).

[372] *See id.*

[373] *Id.*

[374] *Id.*

with all of the data.[375] Critics speculate that Google will likely utilize this data to "discover new markers of health it can apply outside the health care system—across its full suite of products—to infer consumers' medical conditions."[376] Regulators should have asked whether Google was utilizing the data to infer related conditions applied to individuals, which is at least as dangerous as obtaining the data to begin with, if not more.[377]

[125] The opt-in method from the iOS 14.5 update is a strong example of complying with California's Dark Patterns law[378] as it simplifies the process and enables users of all sophistications the choice to grant consent.[379] The Dark Patterns law was necessary to prohibit companies from making it difficult for consumers to opt out of information sharing.[380]

[126] Borrowing from the GDPR's requirement that consent be a clear affirmative act where consumers are opting in for data collection,[381] the iOS update goes beyond showing the consumer a banner informing the user that by utilizing the website they agree to cookies; it requires the clearly affirmative act of clicking on the screen to opt in and agree. Google's opt-out response to the iOS update further reinforces the need for lawmakers to require the opt-in consent model. An industry giant as large as Google will

[375] *Id.*

[376] *See* Marks, *supra* note 371.

[377] *Id.*

[378] *See* Nyhan, *supra* note 332 ("A business's methods for submitting requests to opt-out shall be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out. A business shall not use a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out.").

[379] *See id.*

[380] *See id.*

[381] *See* GDPR, *supra* note 153, at 4(11), 6(1)(a) (defining opt-in consent).

resort to the lowest common denominator—even when pressured by competition—and will not voluntarily request a consumer's consent unless legally required.[382] Thus, the iOS 14.5 update's privacy prompt is a logical example of a consent mechanism that should be incorporated when crafting federal privacy legislation.

C. A Private Right of Action is Necessary

[127] A private right of action is needed to provide individuals the "opportunity to realize their rights in court."[383] A right of action increases the likelihood that businesses who do not comply with the law will be held accountable for their actions.[384] When a government agency is the sole source of enforcement, the focus is typically on big offenders after significant events have occurred.[385] This leaves the rest of the information-sharing world free to exploit consumer data without true consent.

[128] Professor Ari Waldman argues that private rights of action increase privacy law compliance by "forcing organizations to take privacy more seriously than they do now."[386] A private right of action serves as a deterrent, incentivizing businesses to utilize strong data privacy and security practices to avoid litigation.[387]

---

[382] *See* Bennett Cyphers, *Google Says It Doesn't 'Sell' Your Data. Here's How the Company Shares, Monetizes, and Exploits It.*, ELECTRONIC FRONTIER FOUND. (Mar. 19, 2020), https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and [https://perma.cc/QSZ2-ATK3].

[383] *See* Waldman, *supra* note 38, at 831.

[384] *See id.* at 832.

[385] *See, e.g.*, Press Release, Sec. & Exch. Comm'n., Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71 [https://perma.cc/55NR-5NB6].

[386] *See* Waldman, *supra* note 38, at 831.

[387] *See Reclaiming Our Right*, *supra* note 199, at 8.

[129] Big Tech is strongly against providing consumers with a private right of action.[388] The GDPR and CCPA include a private right of action under certain circumstances. The VCDPA and CPA provide for enforcement solely from the state attorneys general. It comes as no surprise that Big Tech has heavily opposed the CCPA[389] that contains more pro-consumer provisions,[390] yet recently supported the VCDPA that contains more pro-business provisions.[391] Big Tech claims that litigation is costly for both businesses and consumers, class actions ultimately benefit the plaintiff's attorneys, and lawsuits can clog up the courts with cases that are ultimately dismissed.[392] However, if Big Tech complies with the federal regulations, the expense should be minimal and considered a cost of doing business.

[130] Other critics argue a private right of action increases litigation.[393] However, a private right of action "is necessary and beneficial to advancing substantive protections for consumers."[394] By allowing private litigation, "development of precedents would lead to the advancement of industry standards."[395] Without a private right of action, only a small number of potential cases are ever investigated, leaving the remaining actors to essentially do as they please. By including the courts in the overall

[388] *See Florida Legislature Misses the Mark on Consumer Privacy Bills*, INTERNET ASS'N. (Apr. 23, 2021), https://internetassociation.org/blog/florida-legislature-misses-mark-consumer-privacy-bills/ [https://perma.cc/4RPM-Y3SX].

[389] *See* Guynn, *supra* note 5.

[390] *See* discussion s*upra* Section IV.A.

[391] *See* Tsukayama, *supra* note 160.

[392] *See Florida Legislature Misses the Mark on Consumer Privacy Bills*, *supra* note 388.

[393] *See Reclaiming Our Right*, *supra* note 199, at 8.

[394] *See id.* at 12.

[395] *See id.* at 21.

enforcement plan, privacy regulation becomes a stronger and more formidable opponent for potentially unscrupulous actors.[396] To mitigate the pressure on the judicial system, the courts should be provided additional resources to handle an increased case load, just like the FTC.

[131] The dual role with the FTC would minimize a private right of action's burden on the courts.[397] According to Waldman, "even an invigorated, aggressive FTC cannot do this alone."[398] A private right of action serves as an additional mechanism for enforcement, when coupled with the FTC, to improve industry compliance.[399] Additionally, a private right of action "improves[s] public trust in businesses through transparency and accountability."[400]

[132] By way of analogy, a private right of action exists under the Civil Rights Act of 1964, allowing individuals to sue for intentional discrimination.[401] "Civil litigation made dangerous machines safer; private lawsuits gave us seatbelts, stronger automobile frames, safer doors, side impact protection, and many other car safety features."[402] If car safety had been enforced exclusively through a regulatory agency, little to no progress would have been made.[403] Thus, a private right of action places businesses on notice that individual events may each result in a challenging court case,

[396] *See id.*

[397] *See id.* at 12 (describing how a private right of action should be utilized in conjunction with other regulatory agencies, such as the FTC, to protect consumers' privacy rights).

[398] Waldman, *supra* note 38, at 830.

[399] *See Reclaiming Our Right*, *supra* note 199, at 8.

[400] *See id.*

[401] *See* 42 U.S.C. §2000d4–a; *see also* 42 U.S.C. § 2000e–5.

[402] Waldman, *supra* note 38, at 831.

[403] *See id.*

instead of a minor report to an agency that will likely not investigate the occurrence. This additional layer of regulation would incentivize businesses to take the regulation seriously and bolster compliance.

D. An Expanded FTC Should Remain the Primary Enforcement Agency

[133] The FTC is currently the primary enforcement agency for federal privacy actions that stem from unfair or deceptive business practices. Over 200 enforcement actions for privacy-related issues have been brought under the FTC's enforcement regime.[404] The minimal resources available require it to focus on only the largest harms and cases with a high likelihood of success.[405] The largest case thus far resulted in an action against Facebook that settled for $5 billion dollars in 2019.[406]

[134] The FTC should continue to investigate unfair or deceptive acts while spearheading enforcement for a new federal privacy law. The FTC already works on numerous cases involving technology providers and employs specifically-trained investigators to understand and decipher complex privacy issues.[407] Lina Khan, a "prominent critic of Big Tech," was appointed as the new FTC chair in 2021. Khan has a background in technology policy and has recently investigated competition among Big Tech platforms.[408] It makes sense for the FTC to continue its enforcement

[404] *See* Goodyear, *supra* note 77, at 79.

[405] *See Reclaiming Our Right*, *supra* note 199, at 13–14.

[406] *See* Goodyear, *supra* note 77, at 79; *see also* In re Facebook, Inc., No. 19-cv-2184, F.T.C. (D.D.C. 2019), https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc [https://perma.cc/Z297-97H2].

[407] Stiefel, *supra* note 215, at 386.

[408] *See* David McCabe & Cecilia Kang, *Biden Names Lina Khan, a Big-Tech Critic, as F.T.C. Chair*, N.Y. TIMES (June 17, 2021), https://www.nytimes.com/2021/06/15/technology/lina-khan-ftc.html [https://perma.cc/5FQY-QJ46].

of privacy issues as the regulatory agency for federal privacy law instead of relying on a patchwork of state attorneys general that may or may not have the specialized knowledge.

[135] With this enforcement authority, the FTC needs the power to specifically write rules to clarify its privacy authority.[409] The current rule-making process is so burdensome that the FTC has not "engaged in it for decades."[410] "This lack of rulemaking authority ensures that, without more, privacy regulation from the FTC will remain vague and technology companies will remain the primary movers in determining what a given legal standard requires."[411] Thus, it is critical that the FTC's rule-making authority be expanded and a private right of action be enacted to provide comprehensive consumer privacy protection.

E. Federal Preemption is not a Concern if the Protections are Strong Enough

[136] Federal preemption of state law is needed to standardize and simplify a federal privacy law. It has been one of the main points lawmakers have disagreed on when contemplating federal privacy laws. Those in favor of federal preemption are concerned with the cost and disruption involved with a business trying to comply with a patchwork of fifty different state laws.[412] Some opponents of the CCPA support federal preemption if it is weaker than the CCPA as a way to ease the current regulation.[413] On the other side, those against federal preemption believe that states should have

[409] *See* Waldman, *supra* note 38, at 828.

[410] *See id.*

[411] *Id.*

[412] *See* Berroya, *supra* note 54.

[413] *See* Guynn, *supra* note 5.

the ability to pass stronger laws, if necessary.[414] Advocates argue that state attorneys general are familiar with the local issues affecting the state's own constituents; however, federal preemption should be examined based on each individual proposal.[415] By including federal preemption in the federal privacy law, states would not be able to pass stronger protections than the federal law without being preempted.

[137] While the CCPA went into effect in 2020, Congress, Big Tech, the United States Government Accountability Office, and the Commerce Department's National Telecommunication and Information Administration have pushed for federal legislation.[416] These entities fear that more states will implement their own privacy statutes, potentially disrupting business and innovation by forcing companies to comply with fifty unique laws.[417]

[138] The issue regarding federal preemption would only come into play if the federal privacy law is weaker than the strongest state law.[418] If federal preemption does not exist, businesses must attempt to determine whether a myriad of rules and exceptions apply to each visitor that happens to click on the website.[419] This could cost businesses excessive amounts of time and

[414] *See* Peter Swire & Pollyana Sanderson, *A proposal to help resolve federal privacy preemption*, INT'L ASS'N PRIV. PROF'LS (Jan. 30, 2020), https://iapp.org/news/a/a-proposal-to-help-resolve-federal-privacy-preemption/ [https://perma.cc/TJ4G-HDW9] (indicating that "privacy advocates emphasize the role that states play in providing new protections for consumers").

[415] *See* Danielle Keats Citron, *The Privacy Policy Making of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 748 (2016) (discussing how "[l]ocal knowledge, specialization, multistate coordination, and broad legal authority have allowed AG offices to fill in gaps" when federal agencies are more constrained by politics).

[416] *See* Guynn, *supra* note 5; *see also* Hendel, *supra* note 17.

[417] *See* Guynn, *supra* note 5.

[418] *See, e.g.*, discussion *supra* Section IV.

[419] *See* Swire & Sanderson, *supra* note 414.

money in continued legal analysis while attempting to comply.[420] Federal preemption would allow companies to structure their compliance based on one law, instead of many state laws plus any additional federal requirements.

[139] Other critics may argue that federal preemption should not exist, and states should be free to pass their own stronger privacy laws. This concern would only come into play if Congress did not set the bar high enough to protect consumer privacy at the federal level.[421] There should be no need for states to invest extensive time and resources into enacting and enforcing their own privacy laws if Congress passes a strong privacy law that requires affirmative opt-in consent and provides consumers with a private right of action. Thus, Congress should enact a federal privacy law that is stronger than any current state privacy law so that federal preemption can minimize business disruption while satisfying privacy advocates and eliminating the excessive burden of complying with multiple state laws.

F. The VCDPA and CPA Should Not Serve as Templates for Federal Privacy Law

[140] While heavily supported by Big Tech for its pro-business features, the VCDPA moves government standards off track from the original FIPPs, models of Notice and Consent, and the constitutionally implied right to privacy.

[141] Big Tech is pushing Congress to model federal privacy law from the pro-business VCDPA.[422] This framework directly conflicts with the iOS 14.5 update results and the strong need for consumer privacy protection. By conforming to the VCDPA, or the watered-down version of the CPA that ultimately passed, regulation would be limited to a narrow group of large

[420] *See* Berroya, *supra* note 54.

[421] *See, e.g.*, discussion *supra* Section IV.

[422] *See* Tsukayama, *supra* note 160.

businesses, leaving a significant segment of the industry unregulated. As previously discussed,[423] the opt-out consent model of the VCDPA would likely have minimal effect on consumers' privacy choices, and the VCDPA lacks a private right of action. To the extent that members of Congress are inclined to model federal legislation off the VCDPA and CPA, perhaps they may be inclined to support stronger privacy protections if they realize how they are personally affected by current data practices.

[142] Prior to voting on any federal privacy legislation, members of Congress would do well to obtain personal information reports from Acxiom,[424] one of the country's largest data brokers. This might drive home the vast quantities of personal data being collected and sold, of which most individuals are unaware. For example, Idaho maintains a repository of adult immunization records.[425] In 2021, legislators became aware their personal information had been collected by the state without their knowledge.[426] Legislators "called on state officials to immediately stop collecting information and destroy any registration information held by the department."[427] As federal privacy legislation has been delayed for decades, a personal discovery of shared information may suggest an urgent need for safeguards that protect consumer privacy rights, in spite of pro-business lobbyists.

[423] *See* discussion *infra* Section IV.C.

[424] *See What Are Data* Brokers, *supra* note 1.

[425] *See* Darin Oswald, *Idaho Republicans: Health officials shouldn't collect immunization records on adults*, IDAHO STATESMAN (Apr. 9, 2021, 2:28 PM), https://www.idahostatesman.com/news/politics-government/state-politics/article250551779.html [https://perma.cc/UT6M-Q272].

[426] *See id.*

[427] *Id.*

VI. PROPOSAL

[143] Congress should draw from the principles of the GDPR, the iOS 14.5 update, and certain features of state privacy law to enact suitable federal privacy legislation. Such legislation should (1) apply to all businesses that collect personal information from consumers located in the United States, (2) require consumers to provide affirmative opt-in consent for data tracking and sharing, and (3) provide a private right of action. The iOS 14.5 update has demonstrated that when faced with a simple, comprehensible choice to opt in to the tracking and sharing of their personal information, only 15% of responding consumers in the United States consent.[428] Apple's iOS update results illustrate United States consumers' interest in protecting privacy and the palpable need for federal privacy regulation. Left virtually unregulated, most online applications and websites will track and share consumer personal data without one's knowledge or consent, subjecting individuals to potential privacy harms like social stigmatization, reputational damage, discrimination, and safety concerns. Thus, a federal law is needed to prohibit businesses from sharing the personal data of unsuspecting consumers for valuable consideration, absent affirmative opt-in consent.

[144] Like the GDPR and state privacy laws, a federal privacy law would include a myriad of definitions and language to provide complete coverage for consumers.[429] This proposal focuses on the most significant elements of the law: (1) to whom it applies, (2) affirmative opt-in consent, (3) a private right of action, (4) FTC enforcement, and (5) federal preemption.

[428] *See* Laziuk, *supra* note 36.

[429] *See* GDPR, *supra* note 153 (showing how the GDPR contains Articles relating to Subject-matter and Objectives, Definitions, Principles Relating to Processing of Personal Data, Processing of Special Categories of Personal Data, Right of Access by the Data Subject, Right to Rectification, Right to Erasure, Right to Data Portability, and Automated Individual Decision-making, Including Profiling).

A. Establishment and Targeting Criterion[430]

[145] The establishment and targeting criterion[431] found in the GDPR should be integrated into federal privacy law. This model should apply to all businesses, without exception, that are either established in the United States or that target individuals currently located therein. Complicated exceptions, allowing smaller businesses to exploit consumer data, should be excluded.

[146] Drawing from the GDPR, a federal law should apply to data controllers and data processors[432] that (1) process personally identifiable information in the context of United States' business activities, regardless of whether the actual processing of data takes place within the United States ("Establishment Criterion"); or (2) target individuals by processing data in conjunction with offering goods or services in the United States or monitoring the behavior of an individual located in the United States ("Targeting Criterion").[433] Like the GDPR, a law should apply to all types of businesses, including online firms and brick and mortar retailers, located both inside and out of the United States. Additionally, it should cover individuals in the United States at the time of data collection, regardless of their official country of residence. There ought not be exceptions for entities the business categorizes as affiliates, as exemplified in the VCDPA, as that title could potentially apply to anyone.[434] A sixty day right to cure provision, as provided in the CPA,[435] should not be included because businesses could

[430] *See* Yallen, *supra* note 134, at 800–03 (describing GDPR's Article 3 requirements as Establishment and Targeting Criterion).

[431] *See* GDPR, *supra* note 153, art. 3.

[432] *See id.* (defining the Territorial Scope).

[433] *See id.*; *see also* Yallen, *supra* note 134, at 800–01.

[434] *See* S.B. 1392, 2021 Gen. Assemb., Reg. Sess., § 59.1-571 (Va. 2021) (describing how a sale of personal data does not include data transferred to an affiliate).

[435] *See* CPA, *supra* note 188.

utilize it as a loophole to violate the law until after an official action has commenced.

[147] Privacy advocates favor provisions that apply to all consumers, regardless of the size or format of the business.[436] Big Tech favors provisions that apply to all businesses that collect and sell consumers' personal information, including data brokers and retail brick and mortar stores.[437] Big Tech also argues that privacy regulation is targeted specifically at large technology companies, as opposed to small businesses that engage in the same practices.[438] Following in the GDPR's footsteps here would provide broad consumer protection while satisfying privacy advocates. This proposal would also satisfy Big Tech's demand for a simplified oversight regime.

[148] The definitions of "sale" and "personal information" are critical in determining what acts fall under this federal regulation. Like the CCPA, a "sale" should be defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[439] In contrast to existing state laws, there should not be exceptions or qualifiers that allow certain businesses to claim exemption from this regulation.

[149] The definition of "personal information" should mirror the CCPA's definition as "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[440]

---

[436] *See* Letter from EPIC, *supra* note 116.

[437] *See* Berroya, *supra* note 54.

[438] *See id.*

[439] *See* Cal. Civ. Code § 1798.140(t) (Derring 2021).

[440] *See* § 1798.140(o).

[150] This law should avoid the potential "service provider" loophole found in the CCPA.[441] The CCPA's service provider exception exempts third-party contractors that receive consumers' personal information from regulation, provided it is for a business purpose.[442] The exempted contractor is not allowed to share or utilize the information for its own purposes.[443]

[151] The scope of the service provider exception is currently being scrutinized in light of Facebook's contention that it is a service provider to which the CCPA does not apply.[444] In contrast, even Microsoft and Google have determined they will comply with the CCPA's requirements nationwide.[445] Facebook argues that it does not charge businesses a monetary amount to install its Pixel tracking cookie on consumers' online devices and that its data collection is "necessary to perform a business purpose."[446] Additionally, Facebook has attempted to shift the CCPA's

[441] *See* § 1795.140(v) (defining a service provider under the CCPA as a "legal entity that is organized or operated for profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose" including a commercial purpose other than performing the purposes specified in the contract and noting businesses are also required to obligate the service provider from further collecting, selling, or using the personal information except as necessary to perform the business purpose).

[442] § 1798.140, (v), (w).

[443] *See* § 1798.145(i).

[444] *See* Eric Westerhold, *Facebook's Attempt to Dodge Compliance with CCPA: We Don't Sell Your Data*, GEO. L. TECH. REV. (2020), https://georgetownlawtechreview.org/facebooks-attempt-to-dodge-compliance-with-ccpa-we-dont-sell-your-data/GLTR-03-2020/ [https://perma.cc/3R24-PCL6].

[445] *See id.*

[446] *See id.*

interpretation onto the businesses that install Pixel by encouraging them "to reach their own decisions on how to best comply with the law."[447]

[152] Privacy experts disagree with Facebook's analysis. Jacob Snow[448] stated that "when a website delivers massive volumes of personal information to Facebook, that's a sale under the CCPA."[449] Professor Chris Hoofnagle[450] believes that Pixel's purpose of the data transfer itself is for "identity and attribution," constituting a sale.[451] Professor Ari Waldman[452] believes Facebook is "taking advantage of some ambiguity in the law to reframe the law's requirements to suit its own purposes" by attempting to claim this "business purpose exception."[453]

[153] Additionally, Facebook claimed the service provider terminology when it made special arrangements with over 150 companies to share more user personal data than it had disclosed.[454] Facebook claimed the entities were considered "extensions of itself—service providers that allowed users to interact with their Facebook friends."[455] "The partners were prohibited from using the personal information for other purposes," according to Steve

[447] *See id.*

[448] *Id.* (Jacob Snow is a technology and civil liberties attorney for the ACLU of Northern California).

[449] *See* Westerhold, *supra* note 444.

[450] *Id.*

[451] *See id.*

[452] *Id.*

[453] *See id.*

[454] S*ee* Confessore et al., *supra* note 278 (discussing how Facebook permitted Microsoft's Bing search engine, Amazon, Yahoo and others to access users' personal information without consent. Facebook even provided Netflix and Spotify access to Facebook users' private messages).

[455] *See id.*

Satterfield, Facebook's director of privacy and public policy.[456] Facebook argued the service provider exception applies to "companies that use the data only 'for and at the direction of' Facebook and function as an extension of the social network."[457] Facebook claimed the service provider exception applied to businesses as diverse as retailers, device makers, and internet search companies.[458] Three former employees of the FTC's consumer protection division discerned that Facebook's "data-sharing deals had probably violated [the 2011 consent agreement Facebook entered into with the FTC]."[459] Violations of the 2011 agreement led to a record $5 billion fine against Facebook in 2019 for "deceiving users about their ability to control the privacy of their personal information."[460]

[154] It is important that federal law further solidify that businesses providing a service cannot utilize consumer personal data for any of their own purposes, including identifying a user or attributing information to a profile about the user. A strong federal law could settle this question once and for all, eliminating the need for continued debates over this exception.

B. Opt-in Consent

[155] Because the requirements of the GDPR have been widely adopted by businesses located in the United States that may reach consumers in the EU, the framework necessary for opt-in consent is already established. Businesses are already utilizing the opt-in framework on a large scale, yet

[456] *See id.*

[457] *See id.*

[458] *See id.*

[459] S*ee* Confessore et al., *supra* note 278 (describing how the consent agreement prohibited "the social network from sharing user data without explicit permission").

[460] *See FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, FED. TRADE COMM'N (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/2NZF-XCAK].

they are not providing the option to United States' consumers because it is currently not required.[461] If a website has not yet implemented this procedure, there are many well-established programs it could utilize,[462] which should minimize disruption in business advancement or excessive cost.

[156] The federal law should draw off the Colorado Senate's original draft by defining consent as:

> "a clear, affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement, such as a written statement, including by electronic means or other clear, affirmative action by which the consumer signifies agreement to the processing of personal data relating to the consumer for a narrowly defined particular purpose. Consent does not include (a) 'acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information'; (b) 'hovering over, muting, pausing, or closing a given piece of content'; and (c) 'agreement obtained through dark patterns.'"[463]

This definition would be ideal because it identifies consent with particularity and specifically describes practices that do not qualify as consent. This is necessary because businesses have implemented similar practices in response to the CCPA,[464] which lead to consumers

[461] *See* discussion *supra* Section V.

[462] *See* Tim Keary, *9 Best GDPR Compliance Software*, COMPARITECH (Oct. 13, 2021), https://www.comparitech.com/data-privacy-management/gdpr-compliance-software/ [https://perma.cc/JH7T-ZJWG] (describing existing software designed to comply with the GDPR's opt-in consent model).

[463] *See* Stauss et al., *supra* note 186.

[464] *See* Akhtar, *supra* note 263.

inadvertently agreeing to the sale of their personal information without their actual informed consent.[465]

[157] A specific Dark Patterns prohibition is necessary to address website designs that "confuse or trick users into opting into selling their information."[466] Dark patterns should be defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice."[467] A federal law should omit the potentially subjective language found in the California Dark Patterns Law that allow businesses to make their own determinations of what constitutes a method that "is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[468] Consumers data initially collected for one purpose may not be utilized for any other purposes in the future without returning to the consumer to obtain affirmative opt-in consent for each additional purpose.

[158] This consent must be expanded to prohibit shadow profiling[469] by specifying that data profiles may not be compiled on individual data subjects who do not have an account with the business,[470] absent a data subject's affirmative opt-in consent.

[159] Apple's iOS 14.5 update has shown that utilizing a simple, understandable prompt, asking a consumer whether they would like their information to be sold or tracked, is an effective mechanism to request

[465] *See id.*

[466] *Id.*

[467] *See* Stauss et al., *supra* note 186 (mirroring the Colorado Senate's original draft).

[468] *See* Nyhan, *supra* note 332.

[469] *See* Solon, *supra* note 40 (noting that shadow profiling occurs when a company creates a profile and collects data regarding a consumer that does not have an account with the company. Facebook has come under fire during Congressional testimony for maintaining shadow profiles on consumers that do not have Facebook accounts).

[470] *See id.*

affirmative, informed consent.[471] The federal law should be structured around the knowledge we have gained from Apple's practices by providing a standardized template to be utilized as a prompt.[472] This prompt should appear prior to initially downloading an app onto a device. It should reappear anytime thereafter when an application wants to track a user's online activities across other apps and websites or sell their information to third parties.

[160] For websites accessed through an internet browser, the federal law should provide a standardized template with the same language as the app that must appear before the website records any data about the consumer or places any cookies[473] onto the device.

[161] For businesses that reach consumers by means other than a website or an app, the federal law should provide a specific template of language that must be provided to the consumer to obtain their affirmative opt-in consent, prior to any collection of personal information.

C. Private Right of Action and FTC Enforcement

[162] The new federal law should be enforced through a private right of action and an expanded FTC with broader powers and more resources. Providing consumers with a private right of action would provide additional incentive for businesses to be concerned with compliance for every single consumer action.[474] The threat of multiple individual cases making their way through the courts—or worse, multiple class actions—should spark additional concern that businesses may be faced with expensive and time-consuming litigation. The FTC could enforce this federal law and continue

[471] *See* Laziuk, *supra* note 36 (Only 15% of U.S. consumers' consented to third party tracking and sharing of personal information when responding to the iOS 14.5 prompt).

[472] *See* discussion *supra* Section V.B.2.

[473] *See* Johnson, *supra* note 321 (defining cookies).

[474] *See* discussion *supra* Section V.C.

enforcing other privacy-related "unfair or deceptive" cases as the centralized regulatory agency for federal privacy law. As privacy and data security has become more crucial to the security and autonomy of United States consumers, the FTC would need to receive a substantial increase in funding and resources to broaden its agency.[475] There might be opposition to this funding from fiscal conservatives. However, the funding would save money in the long run with less reliance on the courts and fewer resources devoted to making and interpreting countless state laws.

[163] Existing departments currently utilized for privacy and technology-related investigations and enforcement should be enlarged. Additionally, the FTC's rule-making authority should be broadened to allow for specific, timely rules to be implemented as necessitated by changes in technology.

D. Federal Preemption to Override State Privacy Laws

[164] While federal preemption has become a widely debated issue, it would not be a concern if the federal law was strong enough.[476] Debates have stemmed from business stakeholders pushing for preemption to streamline their business models and stifle stricter state privacy laws, like the CCPA. Privacy advocates worry that including federal preemption in a federal law that consists of weaker requirements than individual state requirements would provide consumers with less protection.[477] Privacy advocates should be confident that a federal law will effectively protect consumers when it applies to businesses in the same fashion as the GDPR, requires affirmative opt-in consent, and provides a private right of action. Under this proposal, less strict state laws, like the CCPA, would become unnecessary. Therefore, this proposal includes a federal preemption element to override state privacy laws and streamline commerce. This inclusion is meant to promote growth and innovation among businesses without

[475] *See* Unger, supra note 199, at 13–14 (describing how the FTC is currently "resource constrained").

[476] *See* discussion *supra* Section V.E.

[477] *See id.*

creating a web of conflicting, difficult-to-comply-with laws while still providing strong consumer protection.

VII. CONCLUSION

[165] As technology continues to evolve, the need for federal privacy law has never been more essential.[478] The exponential growth of the digital world impacts all consumers in the United States, whether they utilize the internet or not. This must be addressed now, before more damage occurs.[479] The original 2012 proposal of the CPBR was right—consumers do value their privacy.[480] The iOS 14.5 update data should be utilized as a benchmark in drafting privacy legislation that places individuals' privacy rights first, not the wants of mammoth corporations laden with privacy scandals. The American people deserve better.

[166] Congress should draw from the iOS 14.5 update, the principles of the GDPR, and certain features of state privacy law to enact federal privacy legislation that applies to all businesses collecting personal information from consumers located in the United States, requires consumers to provide affirmative opt-in consent for data tracking and sharing, and provides for a private right of action. With proper regulation, technology and innovation can still thrive, without stealing our identities and the representation of "who we want ourselves to actually be."[481]

[478] *See* Drew Simshaw, *Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using Artificial Intelligence in the Practice of Law*, 70 HASTINGS L. J. 173, 207 (2018) (noting that due to rapid advances in Artificial Intelligence, there is an urgent need for ethical guidance because "society cannot afford to wait years for amendments to rules or changes to law").

[479] *See id.*

[480] *See* discussion *supra* Section III.A.3.

[481] *See* Hindi, *supra* note 46.