Seattle Journal for Social Justice

Volume 18 | Issue 2 Article 23

6-2020

Real You Meets Virtual You: It is Time for Consumers to Regain Power Online

Neeka Hodaie
hodaien@seattleu.edu

Real You Meets Virtual You: It is Time for Consumers to Regain Power Online

Neeka Hodaie*

> "This is surveillance and these stockpiles of data serve only to make rich the companies that collect them. This should make us uncomfortable."[1]
>
> – Apple's CEO, Tim Cook, speaking at a privacy conference in Brussels during which he announced, "we at Apple are in full support of a comprehensive federal privacy law in the United States."[2]

I. Introduction

Everyday, our movements online are recorded, analyzed, and used to generate immediate and future profit. Samuel D. Warren and Louis D. Brandeis published their influential article, *The Right to Privacy*, in 1890, "in response to invasions of personal privacy caused by the technological advances of newspapers and photographs."[3] In our current era, the right to privacy may be more appropriately characterized as "knowing what data is being collected and what is happening to it, having choices about how it is

* J.D. Candidate 2020, Seattle University School of Law. Since the start of my law school experience, I have met many inspiring people in the ever-changing privacy and data security Space – I am so fortunate to have such great mentors who continuously inspire me. Thank you to the SJSJ team for the thoughtful feedback on this piece. And a sincere thank you to my family and friends for all their kind encouragement.

[1] Natalia Drozdiak and Stephanie Bodoni, *'This is Surveillance.' Apple CEO Tim Cook Slams Tech Rivals Over Data Collection*, TIME (Oct. 24, 2018), http://time.com/5433499/tim-cook-apple-data-privacy [http://perma.cc/6GQB-EQF3].

[2] James Vincent, *Tim Cook Warns of 'Data-Industrial Complex' in Call For Comprehensive US Privacy Laws*, THE VERGE (Oct. 24, 2018, 05:08am), https://www.theverge.com/2018/10/24/18017842/tim-cook-data-privacy-laws-us-speech-brussels [http://perma.cc/BXS8-5HAZ].

[3] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 HARV. L. REV. 195, 5 (1890).

collected and used, and being confident that it is secure."[4] There is an entire industry around tracking and collecting usage of online platforms.[5] Invasive, constant, and unknown data collection has created comprehensive online identities for every individual user.[6] Generally, the actual individual attached to the online identity that has been stitched together by data collection practices is largely in the dark about their virtual identity.[7] Therefore, individuals who are not even aware of these identities are in no position to be aware of who has access to their comprehensive virtual identity.[8] Businesses are neither encouraging individuals to get to know their online identities, nor are they making accessible the relevant information that is necessary to manage these identities.[9] Our virtual identity is a product of our likes, dislikes, and personal demographics.[10] When consumers are online, the physical cues that alert us that our privacy could be compromised are absent.[11] As technology advances, data collection will continue to grow in

---

[4] Alison M. Cheperdak, *Double Trouble: Why Two Internet Privacy Enforcement Agencies Are Not Better Than One for Businesses or Consumers,* 70 FED. COMMUN. L.J. 261, 263 (2018).

[5] Corporations use third party companies to collect and analyze consumer information. *See* Morgan Hochheiser, *The Truth behind Data Collection and Analysis*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 32, 33 (2016).

[6] *Creepy or Cool?: Staying on the Right Side of the Consumer Privacy Line*, KPMG 17 (2016), https://assets.kpmg/content/dam/kpmg/xx/pdf/2016/11/creepy-or-cool.pdf [https://perma.cc/48VL-RZME] (providing that one leading data broker says it has information on 700 million consumers worldwide and over 3,000 propensities for nearly every US consumer).

[7] *See* Electronic Privacy Information Center, *Online Tracking and Behavioral Profiling*, EPIC,
https://epic.org/privacy/consumer/online-tracking/ [https://perma.cc/24WM-U85B].

[8] *Id.*

[9] *Id.*

[10] Jason Morris and Ed Lavandera, *Why Big Companies Buy, Sell Your Data*, CNN BUS. (Aug. 23, 2012), https://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/index.html [https://perma.cc/D32T-K386] (Acxiom CEO discussing how companies are trying to become intelligent about what consumers might be interested in and who they are).

[11] Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 785 (2016).

sophistication, and our online interactions and movements will face an intensified threat.[12]

In a 2016 survey, eighty-one percent of U.S. respondents stated they "felt that they had lost control over the way their personal data is collected and used."[13] Innovative technology has developed rapidly, making data collection more proficient and intrusive than ever, so the consumer's knowledge of these processes has increasingly fallen behind. While the advancement of technology brings significant benefits for society, our relationship with the internet has changed.

As Tim Cook, the CEO of Apple, said, "technology's potential is and always must be rooted in the faith people have in it."[14] It has become a necessity in our everyday lives. Many essential goods and services are transitioning to online platforms, often exclusively. Online transactions have become extremely efficient, saving time, and often resulting in cost savings. As online transactions increase, the online identities stitched together by our data also become more fully formed. The more a consumer interacts with platforms, the more data is available to be collected about them. Often, online transactions required the consumer to share sensitive information, such as credit card information and an address for shipping and billing.[15] As our levels of connectivity increase, so do opportunities for "every object to serve as continuous surveillance equipment that monitors and collects data about us."[16]

---

[12] *See* Kenneth M. Siegel, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN ST. L. REV. 779, 822 (2007).

[13] Gina Pingitore, Vikram Rao, Kristen Cavallaro, and Kruttika Dwivedi, *To Share or Not to Share: What Consumers Really Think About Sharing Their Personal Information*, DELOITTE (Sep. 5, 2017), https://www2.deloitte.com/us/en/insights/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html [http://perma.cc/5UUN-HTKA].

[14] Vincent, *supra* note 2.

[15] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1379 (2017).

[16] *Id.*

All of the newly established conveniences in our lives, brought to us by the advancement of technologies, come at a price most consumers do not understand.[17] The rapidly changing and innovative nature of online platforms has distracted consumers from gaining a real understanding of what is going on behind the scenes.[18] As technology becomes more precise, the practice and industry built upon snooping on people's daily habits has spread and grown more intrusive.[19]

There is often a great deal of time between when an individual loses their privacy and when that individual realizes the implications of that loss and demands action.[20] Currently, the delay in this understanding has created data sets that are extremely comprehensive and valuable, but which are created by a lack of consumer awareness. Businesses are reaping substantial profits from consumers' oblivious use of platforms.[21] There is an immense market incentive to collect, buy, and sell consumer data; for example, sales from location-targeted advertising reached an estimated $21 billion in 2019.[22] Although consumers certainly benefit from online platforms, and even data collection, such as relevant advertising and free content, the marketplace is better off when consumers are informed about their transactions. How data is collected, processed, and shared is intricate and does not result in a system that an average consumer genuinely understands.[23]

---

[17] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004).
[18] *See Id.*
[19] Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller, and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/JW93-GN5K].
[20] Jay Stanley, *Why Today's Privacy-Invading Online Ecosystem May Not Last*, ACLU (May 31, 2016, 12:30PM), https://www.aclu.org/blog/privacy-technology/internet-privacy/why-todays-privacy-invading-online-ecosystem-may-not-last [http://perma.cc/C2Y8-68Q7].
[21] Schwartz, *supra* note 17, at 2128 (discussing how technology is commodifying personal information).
[22] Devries, *supra* note 19.
[23] Electronic Privacy Information Center, *supra* note 7.

Acxiom, a large data broker, has "approximately 23,000 servers scrutinizing the data of millions of individuals."[24] Once data brokers obtain consumer data, they transfer this information to unaffiliated parties.[25] Acxiom CEO Scott Howe says the company's clients range from small businesses to large Fortune 500 companies.[26] As discussed above, consumers are continually exposing sensitive personal information to businesses online. Consequently, the potential for security risks is substantial. Another 2016 survey found that sixty-four percent of Americans have personally experienced a significant data breach.[27] In light of these countless devastating and wide-ranging data breaches,[28] consumers have started to demand better practices from businesses actively.[29] For instance, studies indicate that consumers desire greater protection and security concerning their data, "but they are also more willing to provide their personal information if companies are transparent about how they intend to use it, allow consumers to easily opt-out of sharing, and provide brief and readily understandable privacy policies and agreements."[30]

Faced with this consumer climate, Congress should pass a law, pre-empting state laws, providing that the consumer must actively "opt-in" for companies to have permission to use the consumer's data and directly market to them, in lieu of the current system in which a consumer is opted-in until that they expressly "opt-out." After a consumer provides "opt-in" consent,

---

[24] Elvy, *supra* note 15, at 1372.
[25] *Id.*
[26] Morris, *supra* note 10.
[27] Elvy, *supra* note 15, at 1381.
[28] Equifax breach exposed information such as full names, birthdates, Social Security numbers, credit card numbers, and driver's license numbers. *See* Thomas G. Jr. Siracusa, *The Equifax Breach: What We Learned and How We Can Protect Consumer Data*, 30 LOY. CONS. L. REV. 460 (2018).
[29] Kevin Cochrane, *To Regain Consumers' Trust, Marketers Need Transparent Data Practices*, HARV. BUS. REV. (June 13, 2018), https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices [https://perma.cc/YZX9-HFK5].
[30] Pingitore, *supra* note 13.

they are sent a standardized email indicating all the information that the company has about the user, explaining how the data will be used, and containing a URL link that directs the system to forget the user's information at any time.

This article thus outlines a plan of action to implement a federal data privacy regulation that will deliver protections for consumers concerning data collection, in hopes of empowering consumers and providing a sense of ownership over their data. Online identities are becoming more comprehensive and intrusive every day, and action to give consumers more power in the data privacy realm is overdue. The protections proposed in this article are necessary due in large part to the highly unequal bargaining power and level of sophistication that surrounds transactions between businesses and individual consumers. Generally, consumers are uninformed regarding data collection and the technology tracking their behavior across platforms to create a sophisticated profile curated to their preferences and habits. Crucially, this regulation will create a market that empowers consumers to take control and become better informed about their online privacy. Consumers cannot begin to comprehend data collection transactions as they are today because the setting in which they take place is mostly invisible and overly complicated. In the future, there should be a trend permitting consumers full visibility of their personal data and how it is monetized.[31] This regulation should aim to make the personal data market more transparent for consumers so that they can make informed decisions about transactions into which they enter and the situations in which they provide consent that allows for their sensitive information to be shared.

This article first introduces the concept of data privacy and the current setting that makes the enactment of federal legislation so crucial. Second, it compares and contrasts opt-in versus opt-out settings, which are generally the two default consumer consent models in the data industry. Third, it

[31] Cochrane, *supra* note 29.

addresses existing United States internet privacy laws and enforcement, and then compares it with the European Union's hefty privacy schemata that was recently implemented, the General Data Protection Regulation.[32] It should be noted at the outset that this article is primarily focused on the regulation of data collection from the beginning of the data transaction. Fourth, this article describes and proposes possible solutions for the necessary components of a comprehensive privacy law in the United States. Lastly, this article addresses various counter-arguments to the recommendations made in this article.

II. BACKGROUND

A. Data Collection and Sharing

The monetary value of personal data is continuing to grow, and corporate America is insistent on profiting from it.[33] The *Economist* magazine stated in 2017 that "the world's most valuable resource is no longer oil, but data."[34] Due to the rising value of consumers' personal data, businesses now view such data as a corporate asset.[35] They, therefore, have worked hard to invest in software that facilitates the most efficient collection of this information.[36] For example, in 2000, when internet toy retailer Toysmart went bankrupt, it planned to sell its customer database to pay back creditors.[37] In light of

[32] *EU General Data Protection Regulation (GDPR)*: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR].

[33] Schwartz, *supra* note 17.

[34] *Regulating the Internet Giants: The World's Most Valuable Resource is no Longer Oil, But Data,* THE ECONOMIST (May 6, 2017), http://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource [http://perma.cc/3TEN-2P8C].

[35] Schwartz, *supra* note 17, at 2057.

[36] Schwartz, *supra* note 17, at 2057.

[37] *See* FTC v. Toysmart.com, LLC (D. Mass. July 21, 2000). "Customer data collected under a privacy agreement should not be auctioned off to the highest bidder," according to Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection." *FTC Announces*

increasing sophistication of consumer data collection, an emphasis has been placed on informational privacy, which is concerned with the use, transfer, and processing of the personal data generated in daily life.[38] Significant asymmetry of information exists in online transactions, and thus an imbalance of power results between data collectors and the subjects of the collection. Further combined with the "systemic disadvantage and the relative vulnerability of consumers" in that market, this culminates in a situation where consumers are not in an ideal position.[39]

Data collection through acquisition is a growing cause for concern. Mergers and acquisitions are taking place with the target of strengthening data sets, and once this data is acquired, it can put a given company in an "unassailable position."[40] Recently, competition regulators around the world have become very interested in the data that large tech companies collect, store, and analyze.[41] A letter from a dozen State Attorneys General to the FTC state concerns about "possible long-term anticompetitive harms arising from the aggregation of 'big data' by a small number of dominant platforms."[42] Acquisitions in digital markets pose risks because of the difficulty in comprehending the future capabilities and harm that could result from combining data sets. There are many strategic rationales for acquisitions aimed almost entirely at the target's data asset, such as combining data sets

---

Settlement with Bankrupct Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, FTC (July 21, 2000), https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding [https://perma.cc/AA5H-DDND].

[38] Schwartz, *supra* note 17, at 2058.

[39] *Id.* at 2078.

[40] David Meyer, *The Privacy and Antitrust Worlds are Starting to Cross Over*, IAPP (Apr. 23, 2019), https://iapp.org/news/a/the-privacy-and-antitrust-worlds-are-starting-to-cross-over/ [https://perma.cc/7E9U-5VUT].

[41] *Id.*

[42] Letter from 12 State Attorney Generals to Donald S. Clark, Sec. of Comm'n, FTC (Oct. 10, 2018), *available at* https://oag.ca.gov/system/files/attachments/press-docs/10.10.2018-multistate-ag-letter-ftc-re-hearings.pdf [https://perma.cc/ZAU4-69UA].

to create more comprehensive profiles on consumers to then sell for advertising or using the data to develop technologies in a market. In the advertising space, the attractiveness and value of a company increase with the amount and detail of user data.[43] The State Attorneys General voiced that

> [a]lthough accumulation of data may generally be procompetitive, there is concern that the immense advantages certain firms have in consumers' data – amplified by network effects attendant to such accumulations – may effectively block new entry or expansion, thereby limiting choice and, in some cases, harming competition. Dominant firms often acquire potential challengers before they become a threat. Some entrepreneurs may feel they have no choice but to sell or close."[44]

For example, Google has recently sought to acquire Fitbit, despite Fitbit's declining share price, for $2.1 billion.[45] Fitbit has amassed the data of over twenty-eight million users—not to mention the established relationships it has with key stakeholders and corporations in the healthcare sector.[46] The U.S. District Court for the District of Columbia stated that "records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic-a vibrant and constantly updating picture of the person's life."[47] Moreover, under current practices, consent legitimizes nearly any form of collection, use, or disclosure of personal data.[48]

---

[43] Bundeskartellam *(Germany's National Competition Regulator)*, Bundeskartellamt Prohibits Facebook from Combining User Data from Different Sources (July 2, 2019), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html?nn=3591568 [https://perma.cc/3H3N-8YMZ].

[44] Letter from 12 State Attorney Generals, *supra* note 41, at 4.

[45] Bridget Diakun, *Google's Acquisition of FitBit Proves that Data is King*, LEXOLOGY (Nov. 15, 2019), https://www.lexology.com/library/detail.aspx?g=ceb8aaa5-f9b0-487f-a50d-3b6cf59f5b01 [https://perma.cc/T7HZ-FRBL].

[46] *Id.*

[47] Klayman v. Obama, 957 F. Supp. 2d 1, 36 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

[48] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013).

Platforms boast about the detailed information they have on the millions of people in their databases to gain business. Focus USA's website states that it has detailed information on 203 million people and over 100 targeted mailing lists, such as "Big-Spending Parents," "First Time Credit Card Holders," "Grown But Still At Home," and "Hi-Tech Seniors."[49] These types of databases contain data about age, gender, income, children, internet connections, and more.[50] Another database, "Hippo Direct, markets lists of people suffering from 'medical maladies,' such as constipation, cancer, diabetes, heart disease, impotence, migraines, and more."[51]

Web pages are no longer static; user clicks are captured, recorded, and monetized—leading to the creation of comprehensive consumer identities based on this information.[52] As aspects of our lives increasingly move to online platforms, a "permanent record of unparalleled pervasiveness and depth" is created.[53] Operators of online platforms generally gather data about what users are doing on their websites; however, some operators also collect data about what the users are doing on other websites through tracking tools.[54] It is possible to monetize all of this personal data in various ways, including targeted advertisements or even sales to hedge funds seeking insights into consumer behavior[55]—and this is all largely unbeknownst to the users that provided it.[56] Through cunning design, privacy-invasive defaults, and take-it-or-leave-it choices, online companies encourage and steer us into

[49] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 22 (Jack M. Balkin & Beth Simone Noveck eds., 2006).
[50] *Id.* at 23.
[51] *Id.*
[52] *Id.*
[53] *Id.* at 26.
[54] Adam Schwartz et al., *New Rules to Protect Data Privacy: Where to Focus, What to Avoid*, ELECTRONIC FRONTIER FOUNDATION: DEEPLINKS BLOG (July 2, 2018), https://www.eff.org/deeplinks/2018/07/new-rules-protect-data-privacy-where-focus-what-avoid [http://perma.cc/C68N-SVCN].
[55] Valentino-Devries et al., *supra* note 19.
[56] Schwartz, *supra* note 53.

sharing vast amounts of information.[57] The result is significant information asymmetry, and thus an imbalance of power; this, combined with the "systemic disadvantage and relative vulnerability of consumers" in that market, has resulted in a situation where consumers are not in an advantageous position.[58]

B. Opt-in System Versus the Current Opt-out System

There are two central concepts regarding consent online: opt-in and opt-out. Opt-in requires the consumer's express, affirmative, or explicit consent.[59] The business bears the burden of getting permission to collect data in opt-in settings.[60] Opt-out assumes that a consumer's lack of action implies consent.[61] Here, alternatively, the burden is placed on the consumer to act.[62] Currently, the vast majority of online interactions rely on an opt-out system, meaning personal data can be collected and used according to the stated privacy policy unless the individual takes steps to indicate otherwise expressly.[63] Opt-out systems make data collection the default, resulting in a collection that is "duplicitous, clandestine, and often coerced."[64] For example, the 1999 Gramm-Leach- Bliley Act allows banks to share personally identifiable data with companies, as long as the privacy statement reserves the right to share the data this way and gives the customer the right

[57] Øyvind H. Kaldestad and Finn Myrstad, *New Analysis Shows How Facebook and Google Push Users Into Sharing Personal Data*, FORBRUKERRADET (June 27, 2018), https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/ [http://perma.cc/W894-2ATE].
[58] Schwartz, *supra* note 17, at 2078.
[59] Jay Cline, *Privacy Consent Glossary*, IAPP (Sep. 1, 2009), https://iapp.org/news/a/2009-09-privacy-consent-glossary/ [http://perma.cc/7WRH-2AR5].
[60] CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 181 (Cambridge Univ. Press, 2016).
[61] Cline, *supra* note 58.
[62] HOOFNAGLE, *supra* note 59, at 181.
[63] SOLOVE, *supra* note 48, at 83-84.
[64] *Id.* at 84.

to opt-out—though sharing with other financial institutions and joint-marketing partners is usually exempt from having to offer that right.[65]

This article will discuss consumer-friendly advantages to an opt-in choice model over the opt-out model that is widely used today. As Jon Leibowitz, a former Commissioner of the Federal Trade Commission recommended, companies should move to a model where "consumers 'opt-in' when it comes to collecting information—especially when it comes to sharing consumer information with third parties and sharing it across various web-based services."[66] Moreover, privacy policies should be easy to understand and should inform the consumer about the type of data the operator seeks to gather, how the operator will use it, how long the operator will keep it, and with whom the operator will share it.[67] The majority of countries favor an opt-in approach.[68] The EU E-Privacy Directive, for instance, requires affirmative consent.[69] In Germany, "double opt-in" is required, meaning a consumer has to agree to receive commercial emails by checking a box and then again opt-in in by clicking on a link contained in the first email received after enrollment.[70] Canada's Anti-Spam Law requires opt-in consent and, in

---

[65] Jennifer Surane, *Google Checking Accounts May Give Banks an Edge in Deposit Wars*, BLOOMBERG (Nov. 17, 2019), https://www.bloomberg.com/news/articles/2019-11-17/google-checking-accounts-may-give-banks-an-edge-in-deposit-wars [https://perma.cc/ZC9C-MBN7].

[66] Jon Leibowitz, Comm'r, Fed. Trade Comm'n, Remarks at FTC Town Hall Meeting on "Behavioral Advertising: Tracking, Targeting & Technology" (Nov. 1, 2007) (*transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/so-private-so-public-individuals-internet-paradox-behavioral-marketing/071031ehavior_0.pdf [https://perma.cc/7QTU-ZX77]).

[67] *See* ADAM SCHWARTZ ET AL., *supra* note 53.

[68] PRIVACY LAW FUNDAMENTALS (2017), available at Bloomberg Law (follow "Practice Centers" tab; then follow "Privacy and Data Security" hyperlink; then follow "Books & Treatises" hyperlink; then follow "Privacy Law Fundamentals" hyperlink), https://www.bloomberglaw.com/product/privacy/pds_home/document/22601411624 [http://perma.cc/L9H3-6FL9].

[69] *Id.*

[70] *Id.*

cases of noncompliance, provides for high monetary penalties as well as a private right of action.[71]

Defaults are powerful and dangerous because of the existence of a large information asymmetry between the consumers and the businesses engaged in data collection.[72] An opt-in rule forces the data processor to obtain consent to acquire, use, and transfer personal information, and therefore works to reduce information asymmetry problems.[73] To operate on an opt-out system is to ignore the blatant unequal power dynamics that govern information transactions.[74] A law that mandates an opt-in system would reduce this culture of automatic data collection and the corresponding consequences.

C. Current Data Privacy Regulation

1. Data Privacy Enforcement

Both the Federal Trade Commission and the Federal Communication Commission have the authority to regulate different aspects of the internet, and individual U.S. states have the authority to enact and enforce their own privacy laws despite the inherently interstate elements of online transactions.[75]

The FCC regulation in this area is relatively new, but the FTC has a longstanding history as the nation's privacy and data security agency, having brought over 500 enforcement actions regarding the privacy and security of customer information.[76] The FTC's Bureau of Consumer Protection is responsible for stopping unfair, deceptive, and fraudulent practices in the

---

[71] *Id.*
[72] Schwartz, *supra* note 17, at 2103.
[73] *Id.*
[74] *Id.*
[75] Alison M. Cheperdak, *Double Trouble: Why Two Internet Privacy Enforcement Agencies Are Not Better Than One for Businesses or Consumers*, 70 FED. COMMUN. L.J. 261, 264 (2018).
[76] *Id.* at 261, 281.

marketplace.[77] Since 1998, the FTC has been the primary enforcer of privacy protection for consumers against companies that violate their own privacy policies.[78] The FTC can issue advisory opinions, promulgate rules, conduct investigations, and initiate administrative or judicial enforcement proceedings under the FTC Act.[79]

The FTC Act[80] gives the Agency two vital powers: prosecution and collection of information.[81] Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[82] A deceptive act or practice is defined as a "material representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[83] An act or practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or to competition."[84]

Through its enforcement authority under Section 5, the FTC has taken up the issue of privacy online without any internet privacy statute.[85] Thus, the FTC can bring civil actions and seek injunctive remedies when it deems that a company has broken a promise it made regarding consumer privacy, whether it be in its privacy policy or design.[86]

---

[77] FED. TRADE COMM'N, *About the Bureau of Consumer Protection*, FTC.gov (last visited April 9, 2020), https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection [https://perma.cc/S5AW-XWZQ].
[78] SOLOVE, *supra* note 47, at 73.
[79] PORTFOLIO 500: FTC PRIVACY ENFORCEMENT, FTC ENFORCEMENT OF PRIVACY AND DATA SECURITY, AN INTRODUCTION, *available at* https://www.bloomberglaw.com/product/privacy/pds_home/document/4544026664 [http://perma.cc/L9H3-6FL9].
[80] 15 U.S.C. § 45 (2006).
[81] HOOFNAGLE, *supra* note 59, at 11.
[82] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[83] Letter from James C. Miller III, Chairman, FTC, to Hon. John D. Dingell, Chairman, Comm. on Energy & Commerce (Oct. 14, 1983).
[84] PRIVACY LAW FUNDAMENTALS, *supra* note 67 at Chapter 9: Consumer Data.
[85] HOOFNAGLE, *supra* note 59, at 38.
[86] SOLOVE, *supra* note 47, at 73.

Although the FTC's work has led to significant progress in internet privacy, companies are primarily regulated based on their compliance with their privacy policies.[87] Because they have the authority to bring actions that is limited to "unfair or deceptive practices," action is generally only taken if a company explicitly lies or misleads in their policies.[88] Currently, the FTC's reach is very limited and is not adequate to protect consumers when companies' stated practices and policies, despite initial disclosures, are unjust. In 2000, for example, the FTC recommended that Congress enact legislation to ensure adequate protection of consumer privacy online because of the proven limited success of self-regulatory efforts.[89] However, Congress has failed to pass comprehensive legislation, and thus self-regulation remains the principal means for addressing issues of consumer privacy today.[90] Without a federal law mandating opt-in consent, companies can continue to use opt-out systems and will not violate the unfair or deceptive act provision as long as they did not state otherwise in their policies. Instead of giving companies large discretion to determine what constitutes reasonable data privacy measures, there should be objective standards for data security.[91]

2. United States Regulation

Unlike the European Union, the U.S. has not enacted a general comprehensive privacy measure. Instead, Congress has passed several narrowly tailored statutes to address particular privacy issues. The way that

---

[87] Christine Bannan, *Equifax's Data Breach Sins Live on to This Year's Tax Season*, THE HILL (Feb. 1, 2018), https://thehill.com/opinion/finance/371815-equifaxs-data-breach-sins-live-on-to-this-years-tax-season [https://perma.cc/S5FC-BUDN].

[88] *Id.*

[89] *Privacy Online: Fair Information Practices in the Electronic Marketplace – A Report to Congress*, FED. TRADE COMM'N (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf [https://perma.cc/5HUX-U9ZK].

[90] Kathryn McMahon, *Tell the Smart House to Mind Its Own Business!: Maintaining Privacy and Security in the Era of Smart Devices*, 86 FORDHAM L. REV. 2511, 2527 (2018).

[91] Bannan, *supra* note 86.

U.S. data security regulations are compartmentalized by each defined sector is ineffective because of the interconnectivity of data and the overarching implications of privacy on all aspects of life.[92]

The Telecommunications Act is an example of a regulation in the U.S. that mandates affirmative opt-in approval instead of passive opt-out practices. The Act requires an opt-in consent system in scenarios where a business seeks to use a consumer's Customer Proprietary Network Information (CPNI)[93] for marketing purposes.[94] CPNI is information that is generated as a result of the customer's telecommunication service.[95] Before the Act, the telecommunication industry was able to sell customers' CPNI data to third-party companies for marketing purposes without the consent of the customer.[96] Initially, Congress left open the definition of what constitutes "approval," and so privacy and consumer advocates believed, or contended, that approval should require express affirmative consent from the consumer, and telecommunications companies argued that a presumption of approval with the option to "opt-out" and withdraw consent would be sufficient.[97]

Later, the FCC further expanded on the Act by stating that there was substantial evidence that an opt-out strategy would not adequately protect customer privacy.[98] The FCC reasoned that, because most customers either do not read or do not understand carriers' opt-out notices, providers would have to obtain "opt-in" consent from consumers before disclosing CPNI to third parties.[99] Today, personal information, similar to CPNI data, is

[92] Jon L. Mills and Kelsey Harclerode, *Privacy, Mass Intrusion, and the Modern Data Breach*, 69 FLA. L. REV. 771, 778 (2017).
[93] 47 U.S.C. § 222(h)(1).
[94] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[95] *Id.*
[96] Electronic Privacy Information Center, EPIC - CPNI (CUSTOMER PROPRIETARY NETWORK INFORMATION) ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/cpni/ [https://perma.cc/2KXP-WCY6].
[97] *Id.*
[98] In re Implementation of the Telecommunications Act of 1996, FCC No. 07-22 ¶ 44 (Apr. 2, 2007).
[99] *Id.*

continuously shared and sold, which is why the opt-in system needs to expand to provide protections to consumers outside of just the telecommunication industry. The various devices we use every day, aside from phones and the information they contain and log, deserve the same type of protection as CPNI.

In contrast, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)[100] fails to include an opt-in requirement but contains one prescribing that a valid opt-out mechanism must be included in commercial emails that are sent.[101] Therefore, the sender of a commercial email is not required to acquire the recipients' consent before sending the commercial email.[102] Until a recipient affirmatively opts-out of receiving future communications, the sender may continue to send these emails to the mailbox of the consumer.[103] The FTC, Federal Communication Commission (FCC), and other agencies enforce the Act.[104] The FCC has increased its enforcement of privacy matters.[105] The email that must contain a valid opt-out mechanism in the CAN-SPAM Act is similar to the email requirement that this article recommends. Companies have been able to implement a process to make opt-out via an email link effective. The mechanisms, therefore, already exist to fulfill the requirement that emails sent by companies must include a link with the right to opt-out.

The Gramm-Leach-Bliley Act (GLBA) regulates data sharing among financial institutions; businesses that are engaged in banking and insuring stocks and bonds, financial advice, and investing while protecting customer

---

[100] 15 U.S.C. § 7704(a)(3)(A).
[101] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[102] CHRISTOPHER BROWN AND LESLEY FAIR, *CANDID ANSWERS TO CAN-SPAM QUESTIONS*, FED. TRADE COMMISSION (AUG. 18, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/candid-answers-can-spam-questions [http://perma.cc/QQT8-N5GL].
[103] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[104] *Id.*
[105] *Id.*

privacy.[106] But this Act is only applicable to financial institutions as defined in the Act.[107] Thus, financial institutions may not disclose customer non-public information to a non-affiliated third-party unless the institution provides or has provided to the consumer a notice that complies with requirements of the Act.[108] An affiliate is any company that controls, is controlled by, or is under common control with another company.[109] The institution can disclose to unaffiliated third parties only if it has clearly and conspicuously disclosed a warning to the consumer that the information they are providing may be disclosed to third parties; the consumer is given the opportunity, before the disclosure of such information, to elect that such information is not disclosed; and the consumer is given an explanation of how to exercise the option.[110] Additionally, in order to share information with a non-affiliated third party, the financial institution must have a contract in place requiring the third party to maintain the confidentiality of the data.[111] Nevertheless, the GLBA does not sufficiently protect consumers because it still follows an opt-out model, and thus an unfair burden is on the consumer to affirmatively prevent companies from sharing their non-public personal information with non-affiliated firms due to the opt-out standard.[112] The opt-out system here continues to take the responsibility off the actors who gain from the disclosure of data and instead puts it on the less informed party, the customer.[113] Consumer inaction implies consent, so the Act allows financial institutions to share customers' personal information unless a step is taken by

[106] *See* 15 U.S.C. §§ 6801-6909 (2010).
[107] *See* Electronic Privacy Information Center, EPIC - THE GRAMM-LEACH-BLILEY ACT, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/glba/ [https://perma.cc/ZQ86-T442].
[108] *Id.*
[109] Id.
[110] 15 U.S.C. §6802(b)(1).
[111] *Supra* note 106.
[112] *Id.*
[113] *Id.*

the customer expressly changing the default.[114] The GLBA errs on the side of economic efficiency over consumer privacy protection. However, it still demonstrates Congressional acknowledgment that consumers are entitled to some level of security concerning their personal information.

In addition to the foregoing, the Children's Online Privacy Protection Act (COPPA) is a federal law governing the collection of children's personal information on the internet, notably requiring parental consent for the collection or use of any personal information of users under the age of thirteen.[115] This Act most closely resembles the legislation that this article proposes. The existence of COPPA demonstrates that our society values the protection of some personal information on the internet. However, the scope of this Act is clearly limited to the regulation of commercial websites and online services directed at children.[116] While covering a more innocent and indeed valuable population, this value needs to extend to protect everyone's personal information and not just that of those under thirteen. All users are at risk of being taken advantage of or being ill-informed about the collection and sharing of their personal information, so greater protections are needed to cover all individuals, regardless of age.

Importantly, COPPA imposes more extensive privacy policy requirements. This includes a link to the site's privacy policy, which must be posted in a visible place on every page where personal information is collected and must include the contact information of the website operators.[117] In addition, it must explain the type of information that is collected, and show information about how it will be used and whether it will

---

[114] *Id.*
[115] Electronic Privacy Information Center, EPIC - CHILDREN'S ONLINE PRIVACY PROTECTION ACT (COPPA), ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/kids/#introduction [https://perma.cc/4SWP-GHH8] (last visited Apr 6, 2019).
[116] *Id.*
[117] *Id.*

be disclosed to third parties.[118] COPPA requires opt-in consent by requiring a website operative to obtain verifiable parental consent for the collection, use, or disclosure of personal information from children.[119] Websites cannot condition a child's participation on the disclosure of more personal information than is necessary for the activity.[120] This requirement safeguards against the potential that businesses could create deceptive loopholes that limit user experiences on their sites and essentially create a no-other-choice option towards sharing.[121] If companies are able to limit and condition consumers' usage of their platforms beyond what is actually necessary to use the site, opt-in consent becomes meaningless. Voluntary consent should involve an actual choice from the consumer, as to whether to accept the terms. Not being able to access the service without agreeing to certain terms does not present a viable choice.[122]

Various federal laws provide very tight control over extremely limited information.[123] Each contains multiple exceptions and loopholes that limit their effectiveness.[124] Privacy law expert Joel Reidenberg notes that the laws are "sectoral in nature, dealing with privacy in certain contexts but leaving gap holes in others."[125] Overall, they fail to address the underlying power relationship involved in this market and therefore are not adequate or satisfactory in addressing today's crucial privacy concerns. The U.S. needs a comprehensive federal privacy law rather than numerous incremental and fragmented laws. As Daniel J. Solove stated, "new privacy problems are not isolated infringements, but are systematic and diffuse."[126] The current inconsistency in privacy law regulation leads to more consumer confusion.

---

[118] *Id.*
[119] 15 U.S.C. § 6502(b)(1)(A)(ii) (1998).
[120] *Id.*
[121] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[122] MEYER, *supra* note 39.
[123] SOLOVE, *supra* note 47, at 71.
[124] *Id.*
[125] *Id.*
[126] *Id.*

Consumers, generally unable to understand which rules apply to their data across various platforms, are likely to mistakenly believe that a choice regarding their data in one area will also protect it in another.[127]

3. State Legislation

Most states have enacted privacy legislation to protect citizens' consumer data. In June 2018, the California legislature unanimously voted into law the California Consumer Privacy Act (CCPA), the most stringent privacy regulation in the country to date.[128]

> The CCPA creates four basic rights for California consumers: (1) a right to know what personal information a business has about them, and where (by category) that personal information came from or was sent;[129] (2) a right to delete personal information that a business collected from them;[130] (3) a right to opt-out of sale of personal information about them;[131] (4) a right to receive equal service and pricing from a business, even if they exercise their privacy rights under the Act, but with significant exceptions.[132]

The Act requires notice, at or before the point of collection, of the categories of collected data and the purposes of collection. Nevertheless, the CCPA still does not require online services to obtain opt-in consent before collecting personal data from users.[133] Additionally, the CCPA does not provide users with an opportunity to opt-out of collection: "[w]hen it comes to users' autonomy to make their own decisions about the privacy of their

---

[127] Steve Pociask, *A Better Way for Online Consumer Privacy*, FORBES (Mar. 23, 2017, 9:04 AM), https://www.forbes.com/sites/stevepociask/2017/03/23/a-better-way-for-online-consumer-privacy/#32d45bf45d04. [http://perma.cc/Y7SL-UXX3].

[128] *About Us*, CALIFORNIANS FOR CONSUMER POLICY (last visited April 9, 2020), https://www.caprivacy.org/about-us [https://perma.cc/SU6D-6UWJ].

[129] *Id.*

[130] While the right-to-know extends to all information a business collected *about* a consumer, the right-to-delete extends to just the information a business collected *from* them. *See* CAL. CONSUMER PROTECTION. ACT *§* 105.

[131] *See* CAL. CONSUMER PROTECTION. ACT *§* 120; *see also* § 140(t) (defining "sale").

[132] CAL. CONSUMER PROTECTION. ACT *§* 125.

[133] *Id.*

data, while notice is a start, consent is much better."[134] The California law is sweeping because of the large scale of the State's economy and the fact that it is not limited in scope to entities that have physical operations in California.[135] Virtually all big tech must become compliant with the CCPA. By passing the CCPA, California, in combination with other States' laws tackling data privacy, show that a privacy movement is spreading throughout the U.S.[136] The CCPA expresses consumers' attitudes and demands for change in the marketplace of their personal data.[137] Because a federal comprehensive privacy law should preempt the California law, it is imperative for an equally strong law, ideally more robust and less ambiguous, to be constructed.

Due to the shifting landscape of consumer demands for privacy online and the emergence of various States' privacy regulations, businesses engaged in data collection and sharing have recently sought refuge in Congress.[138] On one side, privacy advocates are urging Congress to look to the CCPA and the E.U.'s General Data Protection Regulation in creating a federal comprehensive privacy act for the U.S.[139] Unsurprisingly, on the other side,

---

[134] *Id.*

[135] It applies to for-profit entities "doing business" in the state to which any of the following apply: A) Gross annual revenue is in excess of $25 million. B) Annually buy, receive for commercial purposes, sell or share for commercial purposes personal information of 50,000 or more California consumers, households or devices. C) Derive 50% or more of their annual revenues from selling California consumers' personal information. The CCPA also applies to any entity that (1) controls, or is controlled by, a business that meets the above criteria, and (2) shares common branding with that business. CAL CIV. CODE § 1798.140(c).

[136] *How Will California's Consumer Privacy Law Impact the Data Privacy Landscape?*, FORBES (Aug. 20, 2018, 09:30am), https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#y14fc511ae922 [http://perma.cc/T8TQ-GDYQ].

[137] CALIFORNIANS FOR CONSUMER POLICY, *supra* note 126.

[138] Cecilia Kang, *Tech Industry Pursues a Federal Privacy Law, on its own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html [https://perma.cc/356E-RWBQ].

[139] David Pierson, *Amazon, AT&T, Google and Other Companies Say They'd Support Privacy Laws, But There's a Catch*, L.A. TIMES (Sep. 26, 2018, 6:47 AM),

businesses are opposing online privacy laws based on compliance costs, expensive penalties for violations, and restrictive rules on collecting data.[140] The diminishment of user experience online is often cited by companies to governments as the primary reason for not emulating California and Europe's privacy laws.[141]

It is highly ineffective for States to have different and conflicting privacy regulations due to the interconnectedness of the internet, which is why a federal law is necessary. It is unfair for consumers to receive different and, therefore, disparate treatment concerning an inherent right such as data privacy, based merely on their State residence. It is also unrealistic and overly burdensome for companies to comply with various states' individual laws. Policymakers must take care that requirements do not create an unfair burden on smaller-scale companies. To avoid such a burden, Congress should consider tailoring new obligations based on the size and purpose of the service in question.[142] This article does not propose threshold requirements, but it is important to note that they are necessary and should be carefully selected.

4. International Regulation

The European Union's General Data Privacy Regulation (GDPR) went into effect in May 2018.[143] It is far-reaching: applying to any company regardless of the company's location, extending to all those that process the personal data of subjects residing in the European Union.[144] The implications

https://www.latimes.com/business/technology/la-fi-tn-tech-privacy-20180926-story.html [http://perma.cc/B6VC-AXKA].
[140] *Id.*
[141] *Id.*
[142] ADAM SCHWARTZ, *supra* note 53.
[143] *See* Dipayan Ghosh, HOW GDPR WILL TRANSFORM DIGITAL MARKETING HARVARD BUSINESS REVIEW (2018), https://hbr.org/2018/05/how-gdpr-will-transform-digital-marketing (last visited Apr 5, 2019) [https://perma.cc/LX3L-TDXK].
[144] PRIVACY LAW FUNDAMENTALS, *supra* note 67.

are thus massive, felt even in the U.S.[145] Businesses have been implementing the requirements of the GDPR to avoid a potentially large penalty, which can be a fine of up to four percent of annual global turnover or twenty-million euros, whichever is greater.[146] Included in the GDPR are strong consent and opt-in requirements for the processing of personal data.[147] For example, under Article 7 of the GDPR, controllers may only process personal data if the data subject unambiguously consents—and the burden of proof is on controllers.[148]

The U.S. should follow this model. Many companies in the U.S. have already had to alter their practices and implement changes to comply with the GDPR, creating a convenient opportunity for action within the U.S.[149] Because many companies within the U.S. have already implemented the changes, the argument surrounding hardships associated with implementation is weakened.[150]

Furthermore, Article 17 of the GDPR includes a right for consumers to exercise erasure of personal data concerning them without undue delay.[151] The GDPR has created an environment where marketers need to incentivize consumers to share their data by hampering the default preset of automatic data collection.[152] The GDPR aims "to protect consumers' privacy and provide greater control over how their data is collected and used, moreover, the Regulation requires marketers to secure explicit permission for data-use activities within the E.U."[153]

---

[145] Ghosh, *supra* note 141.
[146] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[147] Ghosh, *supra* note 141.
[148] Matthew Humerick, *Taking Ai Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*, 34 SANTA CLARA HIGH TECH. L.J. 393, 405 (2018).
[149] Cochrane, *supra* note 29.
[150] *Id.*
[151] PRIVACY LAW FUNDAMENTALS, *supra* note 67.
[152] Cochrane, *supra* note 29.
[153] *Id.*

III. BETTER PRACTICES

A. Why Opt-In is better than Opt-Out

Black's Law Dictionary defines opt-in as follows: "to choose to participate in something, thus signaling a right of control by an individual."[154] In the current scheme of online interactions between consumers and platforms, notice and choice are foundational principles around which regulation of privacy online has been built. For this reason, consumers encounter dozens of lengthy privacy policies each day. The use of extensive privacy policies as adequate notice for consumers to then make a "choice" about their personal data is built upon a rational choice theory that assumes that individuals can assess the costs and benefits of giving up control over their personal information.[155] However, this assumption is irrational in today's digital era where consumers are bombarded with lengthy privacy policies filled with complicated language, which are ignored and, consequently, because of our inaction, accepted. Notice by means of privacy policies could "only function in a world where there was no scarcity of consumer time and attention," and meaningful choice is only possible where data collection is not the default rule.[156]

A federal data privacy law should be passed that includes mandatory opt-in consent to replace the current opt-out process because opt-in is an affirmative step that signals consent more clearly. Opt-out, by contrast, creates a default rule of consent unless the consumer takes a proactive step to say otherwise, which puts the burden on the less sophisticated party. The way in which the system currently functions "encourages businesses to inflate strategic-behavior costs to increase their own gains, albeit at the

[154] "Opt In," BLACK'S LAW DICTIONARY (10th ed., 2014).
[155] John A. Rothchild, *Against Notice and Choice: The Manifest Failure of the Proceduralist Paradigm to Protect Privacy Online (or Anywhere Else)*, 66 CLEV. ST. L. REV. 559, 614 (2018).
[156] *Id*. at 647.

expense of consumers and the total surplus from the exchange."[157] Furthermore, default rules create a precedent, in which it is less likely that consumers' true intentions are being communicated and respected according to their preferences.[158] An opt-in system creates a sense of entitlement, which a consumer certainly should feel.[159] For example, while explaining the move to an opt-in standard for financial privacy in Vermont, the Banking Commissioner made precisely such an argument, that "instead of waiving their right to privacy by inaction, Vermonters will be protected until they knowingly agree to the sharing of their personal information."[160]

A study found that seventy-five percent of consumers believe that when a website has a privacy policy, it means the site will not share their information with other websites and companies.[161] This evidence points to misconceptions that most consumers have about online privacy. Due to consumers' lack of understanding about the process and system in which their data is being collected and shared, strong consumer protection regulation is necessary. Website and mobile app privacy policies are strategically and knowingly "long, dense, and designed to be as unobtrusive as possible."[162] Data collectors are thus operating by relying on consumers' distorted perceptions about how their personal data is tracked and collected online. In typical commercial settings, silence does not generally operate as

---

[157] Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033, 1101 (1999).
[158] *Id.* at 1102.
[159] Edward Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1244 (2002).
[160] *Id.*
[161] Joseph Turow, Lauren Feldman, and Kimberly Meltzer, *Open to Exploitation: American Shoppers Online and Offline*, ANNENBERG PUB. POL. CEN. OF THE UNI. OF PENN. (June 2005), http://www.annenbergpublicpolicycenter.org/downloads/information_and_society/turow_appc_report _web_final.pdf [https://perma.cc/QVA7-UPC7].
[162] WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 2 (Harv. Univ. Press 2018); *see* Restatment (Second) of Contracts §69 (Am. Law Inst. 1981).

an acceptance of an offer.[163] An opt-in process is the right move towards informed consumer consent with respect to data collection.

Default rules have substantial consequences and should be constructed to place power in the less sophisticated party or at least retain the power that an individual has by virtue of being an individual. Operating under an opt-out system keeps the burden on the less informed party, and benefits the party with superior knowledge.[164] "If the default rule is that inaction equals loss of privacy, then consumers are likely to surrender their privacy in a way that does not reflect their actual preferences."[165] In modern society, time and attention are scarce resources for consumers; and generally, default decisions have been created to reflect these values.[166]

Research has shown that users rarely change pre-selected settings.[167] In many cases, both Facebook and Google have set the least privacy-friendly choice as the default.[168] The design and language used in Facebook's privacy controls have been found to nudge people toward sharing the maximum amount of data with the company.[169] Due to the significant disparity in the bargaining power between the consumer and data collectors, affirmative steps must be taken to give more power to consumers; the default rule of opt-out does the exact opposite. As companies with some of the largest collections of consumer data expand into more industries, such as Google's

---

[163] Sovern, *supra* note 155, at 1105.
[164] Janger & Schwartz, *supra* note 157, at 1241.
[165] Sovern, *supra* note 155, at 1094.
[166] HARTZOG, *supra* note 160, at 53.
[167] Solove, *supra* note 47, at 1884.
[168] *Id.* Yet, some might say that "[g]iven the value of personal information, it would be surprising if companies did not strategically leverage framing to get people to disclose more." HARTZOG, *supra* note 160, at 42.
[169] Allen St. John, *CR Researchers Find Facebook Privacy Settings Maximize Data Collection*, CONSUMER REPORTS (June 27, 2018), https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/ [https://perma.cc/5PMS-5P9E].

creation of its heath division[170] or Big Tech's expansion into financial institutions, sensitive consumer data is even more at risk and should not be subject to automatic data collection as the default. These companies have the potential to use their troves of data to increase their expansion in these spaces rapidly.

Reasonable limits should nevertheless also exist on the opt-in consent system to ensure it does not become overly burdensome or inefficient for the consumer. For example, opt-in consent might not be required for a service to take steps that the user has requested, like collect a user's mailing address from shipping them the package they ordered.[171] However, even in situations where an affirmative opt-in is not required, the service should always give the user clear notice of the data collection and use.[172] This is especially true when the proposed method is not part of the transaction, "like renting the shipping address for junk mail."[173]

Sophisticated technology, coupled with confusing legalese, creates a situation where individuals are severely outmatched.[174] Pam Dixon, executive director of the World Privacy Forum, stated, "the deck is stacked…it takes an extraordinarily diligent consumer to make informed privacy choices on Facebook."[175] Professor Woodrow Hartzog urges that "privacy law should ask whether a particular design interferes with our understanding of risk or exploits our vulnerabilities in unreasonable ways with respect to our personal information."[176] The overwhelming unequal

[170] Jeremy Kahn & John Lauerman, *Google Taking Over Health Records Raises Patient Privacy Fears*, BLOOMBERG LAW (Nov. 21, 2018), https://www.bloomberg.com/news/articles/2018-11-21/google-taking-over-health-records-raises-patient-privacy-fears [https://perma.cc/U7FU-UYSM].
[171] ADAM SCHWARTZ, *supra* note 53.
[172] *Id.*
[173] *Id.*
[174] HARTZOG, *supra* note 160, at 53.
[175] CR RESEARCHERS FIND FACEBOOK PRIVACY SETTINGS MAXIMIZE DATA COLLECTION (last visited Oct. 7, 2018), https://www.consumerreports.org/privacy/cr-researchers-find-facebook-privacy-settings-maximize-data-collection/ [http://perma.cc/S9ZK-C3BZ].
[176] HARTZOG, *supra* note 160, at 145.

bargaining power between the parties, stemming from consumers' unawareness of data collection and sharing practices, is precisely why the law must provide special safeguards to protect consumers.

B. Standardized Email

This article proposes a second layer of protection via a standardized email that is sent after a consumer opts-in. Specifically, the standardized email should clearly list all information that has been collected and stored about the user and describe it in easy-to-understand terms, and delineate how and what the data will be used for, ideally serving to put the consumer on meaningful notice. Within the standardized email requirement, it should be mandatory that a link exists that enables the user to exercise a "right to be forgotten," based on that in the E.U.'s GDPR, at any time. The email enables a consumer to more easily reference the "contracts" that they enter into with providers to share their data. As is, even when a consumer is asked for affirmative consent, there are few traces of the relationship they just entered with the provider whose box the consumer ticked. A fundamental flaw exists without this email: a user who agrees with contract terms by ticking a box never receives a copy of the relationship terms. Thus, consumers are subject to a transactional relationship that they may not even be able to reference later.

The follow-up email is valuable as a means of record collection so that consumers can retain the consent they have given. Users are continually engaging with online platforms, and are unlikely to remember the sites and companies they have allowed to collect and share their data. It is important for consumers to have a record of the "transactions" that they have entered into. In light of the massive security breaches, the FTC has filed complaints, and made public announcements of bad practices, stating consumers need to be able to check whether they have shared information with a specific platform.

Additionally, the email requirement will, therefore, work to increase transparency about precisely what information the consumer has shared and

how it will be used. The consumer will be on notice and alerted by the email in a more meaningful way because it will contain their shared information for the consumer to see. Additionally, the email will make it possible for consumers to maintain records and monitor with whom they opted into sharing information and for what purpose. This creates increased transparency in a currently invisible and disappearing transaction in which personal data is shared.

Ideally, consumers will spend time actually looking over privacy terms when they are put forth in simpler terms and their personal information is clearly displayed with the notice that it has been shared and stored with others as well. The email requirement serves as a reminder to consumers to take control and understand the use of their data.

The standardized email is positive for businesses too. It will create a space for companies to compete in the domain of consumer privacy because this requirement will provide for a more simplified means to compare the data collection policies of the various businesses that the consumer has elected to opt-in and share information with. This may incentivize data collectors to conform to consumer-friendly norms across the spectrum because, ideally, the standardized email will assist consumers in becoming more knowledgeable about data collection practices and recognizing egregious terms and practices. Ultimately, the mandatory standardized email should incentivize companies, which are competing with one another, to adopt higher, more sensitive best practices for consumers in regard to data collection and sharing. Additionally, data collectors should see the standardized email as an extra layer of protection for themselves as well, as evidence shows that businesses that neither tell customers how they use their data nor offer any control are at greater risk of financial harm after a data

breach.[177] With more transparency, both sides of the transaction are more protected.

1. Right to be Forgotten

The required "right to be forgotten" link within the email will give consumers more control over their data and will give providers a process for the consumer to change their mind about the consent they initially provided. Consumers should feel in control of the data transaction at any stage, rather than just at the beginning—since the asset is their personal information. Article 17 of the GDPR states as follows:

> (1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
>
> > (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
> >
> > (b) the data subject withdraws consent on which the processing is based… and where there is no other legal ground for the processing…[178]
>
> (2) Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such

[177] Kelly D. Martin, Abhishek Borah, and Robert W. Palmatier, *Research: A Strong Privacy Policy Can Save Your Company Millions*, HARV. BUS. REV. (Feb. 18, 2018), https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions [http://perma.cc/TK4C-T2AM].

[178] *See* GDPR, art. 17(1)(c)–(f) for more situations that trigger the right to be forgotten.

> controllers of any links to, or copy or replication of, those personal data.[179]

Furthermore, the third paragraph states exceptions to the right to be forgotten that are created in the above provisions; and of crucial importance is Article 17(3)(a), which creates an exception when the right to be forgotten comes in conflict with "the right of freedom of expression."[180] In the case that the lawful basis for processing is either a legitimate interest for the controller or public interest, a balancing test is appropriate; the data controller will weigh and balance the data controller's legitimate interest or the public's interest in having access to the information versus the data subject's fundamental right to privacy.[181] However, deletion is mandatory when the data subject requests removal upon the legal basis of consent.[182] The GDPR is an apt example of a right to be forgotten that empowers consumers with protection while still having restrictions and limitations that best serve the public interest.

Individuals' ownership over their personal data should be continuous—the right to be forgotten requires a shift in the current ideology that once control over privacy is exchanged at the initial encounter of the relationship with a business, it is from that point on lost to the consumer for future purposes.[183] Currently, even the California Consumer Protection Act, the most rigorous data protection regulation in the U.S. does not have the same reach as the E.U.'s right to be forgotten.[184]

---

[179] GPDR, art. 17.
[180] *See* GDPR, art. 17(3)(a)–(e).
[181] Shaudee Dehghan, *How Does California's Erasure Law Stack Up Against The EU's Right to be Forgotten*, IAAP (Apr. 17, 2018), https://iapp.org/news/a/how-does-californias-erasure-law-stack-up-against-the-eus-right-to-be-forgotten/ [http://perma.cc/7WRH-2AR5].
[182] *Id.*
[183] Fiona Brimblecombe and Gavin Phillipson, *Regaining Digital Privacy: The New Right to Be Forgotten and Online Expression*, 4 CAN. J. COMP. & CONTEMP. L. 1, 20 (2018).
[184] BakerHostetler Law Firm, *The California Consumer Privacy Act: Frequently Asked Questions*, BakerLaw, https://bakerlaw.com/webfiles/Privacy/2019/Briefs/California-Consumer-Privacy-Act-FAQs.pdf [https://perma.cc/A5U4-8MMK].

The proposal in this article incorporates the GDPR's right to be forgotten into the mandatory standardized email, which is required to be sent any time consumer information is collected, stored, or shared. It is important to note that exceptions to the right to be forgotten are needed—to allow for the free flow of information, which is necessary to comply with the freedom of individuals and the public at large. Congress should be careful when crafting exceptions to the right to be forgotten in order to avoid challenges of unconstitutionality. At the same time, exceptions must be narrowly tailored to avoid loopholes that could sacrifice consumers' right to be forgotten.

It is difficult for the average consumer at the time of data collection to make a rational judgment about future privacy implications because the implications are usually unknown at that time.[185] The right to be forgotten, contained in email form, eliminates the burden of having to remember and search every platform that a consumer interacts with in order to exercise control. The option to be forgotten will be available in a consistent manner throughout all platforms that collect, store, or share, consumer data. In circumstances where a consumer is able to obtain the necessary information needed to opt-out, the cost in time and money of communicating and negotiating with the relevant information gatherers is substantial.[186] It is very difficult to opt-out, if only because it is incredibly challenging to have a recollection of the places where one had opted-in. Documenting all the platforms to which the consumer has given consent for data collection will create a log, which will make it more practical for a consumer to keep tabs on and update preferences or exercise the right to be forgotten. This right incentivizes companies to maintain rigorous controls and appropriate policies because they do not want to lose the consent they once received from a consumer. Additionally, the standardized form of the email remedies the

[185] Solove, *supra* note 47, at 1902.
[186] Sovern, *supra* note 155, at 1075.

issue of manufacturing designs purposefully or inadvertently making opt-out difficult or hard to understand on some platforms.

A consumer may exercise the right to be forgotten at any time, which empowers consumers with a sense of control over their data beyond just the initial stage. In this way, "[a] right of exit prevents initial bad bargains from having long-term consequences."[187] Studies show that "people are more likely to opt-in if they feel they have the ability to change their mind and refuse further use and transfers of personal information because then the choice is not permanent."[188]

IV. ENFORCEMENT

The Federal Trade Commission should assume the role of enforcement of this legislation due to the Commission's unparalleled experience in protecting consumers in the market through its Bureau of Consumer Protection and Bureau of Competition. The FTC has been at the forefront of privacy enforcement, and is in the best position to carry out the enforcement of a comprehensive privacy regulation in the U.S. Whether by examining mergers and acquisitions to prevent harm to consumers, or by looking at unfair and deceptive practices by businesses, the FTC is continually checking on the market as its knowledge of privacy is the broadest in the U.S.[189] In 2006, the FTC started hiring technologists to advise its lawyers on new technology.[190] The FTC currently brings legal actions against organizations that have violated consumers' privacy rights by charging defendants with violating the FTC Act, but it also enforces other federal laws relating to consumer privacy and security.[191] Some sectors are expressly exempt from

[187] Schwartz, *supra* note 17, at 2106.
[188] *Id.* at 2105.
[189] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583 (2014).
[190] HOOFNAGLE, *supra* note 59, at 67.
[191] FTC page on Privacy and Security Enforcement, where press releases are available, which includes complaints and settlements. *See* Federal Trade Commission, *Privacy and*

Section Five of the FTC Act, meaning that the FTC cannot bring Section Five actions or investigations against financial institutions, airlines, telecommunications carriers, and others.[192] Therefore, any legislation that is passed should expressly grant enforcement authority to the FTC, so that the Commission is not constrained by Section five. The statutes discussed above, as well as others,[193] all grant enforcement authority to the FTC.[194]

Further, a sweeping act such as this should bring more funding to the Commission and thus incentivize it to expand its internet privacy division, which seeks "to protect consumers' personal information and ensure that consumers have the confidence to take advantage of the many benefits of products offered in the marketplace."[195] The FTC has played a significant role in leading suits against giant corporations while allowing innovative business practices. It is vital for an organization to be accountable for its data processing activities. So the inclusion of a substantial penalty, enforceable by the FTC, is absolutely necessary to make this type of regulation capable of success.

V. COUNTER-ARGUMENTS

Opponents of data privacy laws generally believe that self-regulation is the best means for internet regulation. Though, the current climate of intrusive data collection and devastating data breaches has proven otherwise. The CEO of Apple, Tim Cook, has voiced his opinion in support of privacy regulation;

Security Enforcement, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement [https://perma.cc/C6NE-5Q8V].

[192] PRIVACY LAW FUNDAMENTALS, *supra* note 67.

[193] *See infra* discussions of the FTC Act, COPPA, and the Gramm-Leach-Bliley Act; *see also* the Telemarketing and Consumer Fraud Abuse Prevention Act (TCFAPA), 15 U.S.C. §§ 6101-6108; and the Fair Credit Reporting Act (FCRA)., 15 U.S.C §1681.

[194] PRIVACY LAW FUNDAMENTALS, *supra* note 67.

[195] FED. TRADE COMM'N, *Privacy & Data Security: Update 2017* (2018) https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf [http://perma.cc/M27V-8Y96].

"I'm a big believer in the free market, but we have to admit when the free market is not working, and it hasn't worked here."[196] Critics complain opt-in requirements would create a costly burden on the business that exceeds the value of consumers' opting in.[197] It is often the case that when changes to consumer law are proposed, the estimated cost burdens are widely inflated.[198]

In the midst of growing consumer skepticism about data collection practices, an opportunity to build consumer trust has presented itself. Companies can build customer value by implementing a more transparent process by which they collect data. When consumers are allowed to opt-in to data collection and sharing, they are given a meaningful choice instead of a default rule for sharing and collection. Businesses view consumer privacy as a compliance obligation, which has led to missed opportunities for businesses to recognize that the protection of personal information can be used to differentiate a company from its competitors.[199] Businesses should consider how information management practices can significantly affect brand equality given the increased consumer focus on the protection of personal information.[200] A change to opt-in systems enables companies to continue to collect data from willing consumers while also ensuring that their customers have meaningfully consented to the risks of a future security breach when they read the acknowledgment.

It is in the best interests of businesses to implement privacy policies that provide consumers with transparency and control. One Harvard Business Review study supports this claim, noting in particular that "a good corporate privacy policy can shield firms from the financial harm posed by a data

[196] Mike Allen and Ina Fried, *Apple CEO Tim Cook Calls Our Regulations "Inevitable,"* AXIOS (Nov. 18, 2018), https://www.axios.com/axios-on-hbo-tim-cook-interview-apple-regulation-6a35ff64-75a3-4e91-986c-f281c0615ac2.html [http://perma.cc/MX6P-7PW5].
[197] Sovern, *supra* note 155, at 1106.
[198] *Id.* at 1113.
[199] David Hoffman, *Privacy Is a Business Opportunity,* Harvard Business Review (last visited April 18, 2020), https://hbr.org/2014/04/privacy-is-a-business-opportunity [https://perma.cc/636N-9RSY].
[200] *Id.*

breach—by offering customers transparency and control over their personal information."[201] Furthermore, the study's research showed that sometimes data breaches can create beneficial competitive effects.[202] For instance, following the massive Anthem data breach in 2015, rival Aetna gained about $745 million on the day of the breach due to competitive effects.[203] As the study goes on to show, companies that provide high levels of data transparency and control would be protected from data breaches but also would be shielded from spillover effects if a close competitor experienced a data breach.[204] Conversely, companies not providing high levels of transparency and control are at risk not only if they suffer a breach, but also if a competitor does.[205] It is thus essential to all actors that companies standing to make a profit from consumer data are required to inform individuals about the unseen consumer data marketplace. Moreover, a majority of companies have already implemented many of these processes in their push to become compliant with the GDPR, so the burdens are lessened. For many this change would merely mean an expansion of already implemented procedures for E.U. consumers to U.S. consumers. Due to GDPR implementation that has taken place over the past several years, brands have an opportunity to reevaluate data practices, engage in better communication to customers, demonstrate their commitment to their privacy promises, and, thus, come out stronger on the other side.[206]

Second, critics argue that many data collection practices create better user experiences for consumers, such as targeted advertisements, and data collection has many beneficial attributes for technology innovation.[207] Data collection allows the advertisements we are shown on various platforms to

[201] Martin, *supra* note 175.
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] Ghosh, *supra* note 141.
[207] Morris, *supra* note 10.

be tailored to our interests.[208] There are lots to be gained from this argument, as advertising revenue is the chief revenue for many technology companies. Google's advertising revenue from 2019 was $134.8 billion dollars, 83.9 percent of Google's total revenue.[209]

Although targeted advertisements are, for some, advantageous in many ways, gaining this information through deceptive measures that most consumers do not understand is not the proper way to do it. First, under an opt-in system, consumers who like targeted ads can still make the meaningful choice to share their data. This practice will not be eliminated; users will always be able to balance and decide what is important to them. Further, that argument "overlooks the ability of businesses to persuade consumers, an ability that powers our current marketing environment."[210] Indeed, businesses have extraordinary capabilities to successfully market to their ideal consumer bases, shown by businesses' proclivity to thrive via more traditional means before the era of targeted ads. An opt-in system gives businesses an incentive to clearly explain to consumers, at the time of the decision, the benefits and consequences of participation.[211] This article thus advocates that if, after given the information to make a decision, the consumer understands what they are giving up and still decides against opting in, the choice should simply be respected.[212]

VI. CONCLUSION

The time has come for the enactment of a robust federal privacy framework that should preempt state law and put consumers in control of their online identities. The recommendations made in this article do not suggest an end to data collection. Of course, the businesses engaged in data collection are

[208] *Id.*
[209] Alphabet Inc., Annual report (Form 10-K), at 30 (Feb. 3, 2020).
[210] Sovern, *supra* note 155, at 1118.
[211] *Id.* at 1106.
[212] *Id.*

highly sophisticated and are very knowledgeable about the benefits of consumer data. The hidden and mostly invisible nature of the consumer personal data marketplace limits the potential for consumer action and removes an incentive for companies to restrict their commercial use of such information.[213] It is irrational to think that consumers can adequately protect their personal information and make meaningful choices regarding data collection when they are mostly unaware of how companies use their data.[214] The financial incentives and value associated with data collection and sharing encourage businesses to design and employ platforms that achieve the most optimal consumer data.[215] By mandating rules regarding consumer consent, requiring a record of the collection, and providing an easy-to-access option to exercise the right to be forgotten, the highly imbalanced power dynamic in the data transactions taking place every day is given some relief.

No single comprehensive privacy law exists in the U.S.; privacy rights come from an assortment of sources—the U.S. Constitution, state constitutions, federal and state statutes, and common law.[216] The final objective is to establish a law that empowers consumers to have greater participation and control over their personal data at all stages.

The proposals made in this article are intended to empower consumers by requiring users be informed and have choices at the beginning, the middle, and at the end of the transaction to allow companies to collect and share their data. Through the instruments of mandatory opt-in consent, standardized follow-up emails, and an easy-to-access right to be forgotten at any time, consumers will be given more protection. The opt-in requirement will eliminate the default rule of automatic data sharing and collection and will place the burden on the appropriate party, the business who stands to profit

---

[213] *Id*. at 1072.
[214] *Id*. at 1074.
[215] HARTZOG, *supra* note 160, at 5.
[216] Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERK. TECH. L.J. 497, 508 (2002).

for the sharing and collection. The requisite standardized email provides a type of double-layer protection for the consumer as the more vulnerable and less sophisticated party. The email also increases transparency regarding information the consumer has shared and how this information will be used. Additionally, the email will function in such a way that allows the consumer to maintain records and monitor the actors with whom they opted into sharing information, thus allowing them to check whether they had shared information with that company in the event of security breaches or bad practices that are announced after-the-fact. Finally, the email will contain a link that allows users to opt-out and cease sharing information with the company at any time.

As web services continue to grow in sophistication, so will their profits. The current patchwork privacy regulation has failed consumers. While the practice of data collection and sharing will continue and likely increase as technology advances, the correct regulation would promote transparency and give more control to consumers. A federal regulation is needed to set a benchmark within the industry as it continues to grow exponentially. Ideally, once consumers are given the correct tools to understand better and take control of their data, they will be in an improved position to demonstrate their actual market demands and desire.