THE CASE AGAINST REGULATION OF PRIVATE CONSUMER DATA

KEVIN TANG*

Abstract

With societal dependence on technology at an all-time high, the collection and dissemination of user data by technology companies has come under intense scrutiny by politicians and the public alike. Federal privacy laws in the United States operate on a piecemeal approach, with vulnerable populations and sensitive data garnering specific privacy protections. Absent these categories, the default laws for privacy are based on the contractual relationship between the data collector and the data provider, which de facto allows technology companies to self-regulate their data collection and dissemination practices. While the prospect of allowing industry to self-regulate vast amounts of user data encompassing much of daily life seems alarming, this is nothing new to the industry and additional regulation may not necessarily be warranted.

This Note argues that pushes for regulation should be limited, and if necessary, cautiously undertaken. This Note examines the current regulatory framework governing data privacy and its effectiveness. This Note then challenges prominent reasons for increasing privacy regulation. Finally, this Note makes alternative policy recommendations that could alleviate privacy concerns without the costly burdens of sweeping federal legislation on the industry and consumers.

* Boston University School of Law, J.D. 2021; University of Illinois, Urbana-Champaign, B.S. 2016. The author would like to thank the staff of the *Review of Banking & Financial Law* for editing this note and Professor Gary Lawson for his feedback and thoughts.

Table of Contents

I. Introduction

In mid-January of 2020, Alphabet became the fourth American company, behind Apple, Amazon, and Microsoft, to hit $1 trillion in market capitalization.[1] These four companies combine for an astonishing seventeen percent of the entire value of the Standard and Poor's (S&P) 500.[2] The machine largely responsible for funding and propelling these companies to record highs is user data-based advertising (Behavioral Advertising).[3]

Behavioral Advertising is the use of a user's past history to predict that user's tastes and preferences in order to target them with

---

[1] Michael Sheetz, *Apple, Amazon, Microsoft and Alphabet Have Traveled Similar Paths on the Road to $1 Trillion*, CNBC (Jan. 31, 2020, 1:42 PM), https://www.cnbc.com/2020/01/31/apple-amazon-microsoft-and-alphabet-and-the-road-to-1-trillion.html [https://perma.cc/53QF-U7SH] (chronicling the rise to surpass one trillion dollars in market capitalization of Apple, Amazon, Microsoft, and Alphabet).

[2] *Id.* ("Combined, the four trillion-dollar companies—Apple, Microsoft, Amazon, and Alphabet—make up 17% of the S&P 500's total market value ….").

[3] Eric Rosenberg, *How Google Makes Money (GOOG)*, INVESTOPEDIA (Dec. 5, 2018), https://www.investopedia.com/articles/investing/020515/business-google.asp [https://perma.cc/4LDL-SH6T] ("A staggering $24.1 billion of Google's $27.7 billion revenue for Q3 2018 was from advertising ….").

specific advertisements.[4] The specific process involves a website or internet service provider (ISP) creating a profile on a user based on what services they use and what information they look up.[5] Once these profiles are created, the website or ISP can sell this information directly to third-party advertisers who then use it to target that profile with relevant advertisements.[6] It is important to note that generally, the information collected does not include personally identifiable information—rather the profile created is typically generated based on using either cookies or deep packet inspection.[7] Cookies are data sent from websites to web browsers which store the data under uniquely assigned ID's.[8] For example, an online shopping site will store cookies on your browser so that if you leave the site and come back, your shopping cart remains full.[9] Users can "turn off" cookies on their web browsers, but almost all websites use cookies and many will not run without cookies.[10] Deep packet inspection involves an ISP examining all the internet traffic to and from a user's IP address.[11] This method is considered more invasive as there is no way for users to opt out; however, deep packet inspection is only used for around ten percent of U.S. internet users.[12] The sheer size and breadth of the data collected from

---

[4] Katherine J. Strandburg, *Free Fall: The Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 99–100 (2013) (comparing behavioral advertising, which utilizes "large-scale and long-term" data collection, with undirected and contextual advertising).

[5] Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUT. & HIGH TECH. L.J. 3, 4 (2011) (describing how ISPs compile personal data into consumer profiles to target advertisements).

[6] *Id.* at 22 ("[P]rofilers often share the data they collect about consumers.").

[7] *Id.* at 7 (explaining that cookies and deep packet inspection are among the primary methods for building consumer profiles and illustrating how this is done with cookies in a way that avoids using personal identifiers).

[8] *Id.* at 7–9 (giving a detailed explanation of how cookies generally function and how advertisers form networks of hundreds or thousands of websites that will share cookies).

[9] *Id.* at 8–11 (describing how cookies can be used to remember items in an online shopping cart between visits through communication with the web browser).

[10] *Id.* at 11 (illustrating how cookies are commonly used to operate website processes).

[11] *Id.* at 12–15 (describing how ISPs can use deep packet inspection to build customer profiles).

[12] *Id.* ("[T]his method of profiling is practically impossible to stop or avoid.").

users[13] mixed with the fact that Behavioral Advertising necessarily requires "large-scale and long-term collection, storage, analysis, and, in some cases, sharing of data about Internet users"[14] raises concerns among privacy advocates and regulators.

The push to regulate the collection and dissemination of user data has been around since the use of personal computers became more widespread in the late 1980s.[15] Since then, public support for such regulation has fluctuated, but has been rising recently following events like the Equifax data breach and Facebook's Cambridge Analytica scandal.[16] While those events deal with the dissemination of highly sensitive information, the calls for regulation expand beyond that sphere and seek to regulate the mere collection of securely held data, freely given by users.[17] This has culminated in California passing and recently implementing its new data collection law, the California Consumer Privacy Act (CCPA), which is loosely based on the European Union's (EU) own recent data protection law, the General Data Protection Regulation (GDPR).[18]

The CCPA applies to any for-profit entity servicing California residents that: (1) earns more than $25 million in annual revenue; or (2) has personal data on more than 50,000 consumers; or (3) collects more than half their revenue from the sale of personal data.[19] Notably,

---

[13] Jana N. Sloane, Comment, *Raising Data Privacy Standards: The United States' Need for a Uniform Data Protection Regulation*, 12 J. MARSHALL L.J. 23, 42–44 (2019) (observing that data brokers like Acxiom has data on 1 billion cookies and mobile devices, while Oracle provides access to 5 billion "unique" consumer IDs).

[14] Strandburg, *supra* note 4, at 99–100.

[15] David Ruiz, *US Congress Proposes Comprehensive Federal Data Privacy Legislation—Finally*, MALWAREBYTES LABS (Mar. 28, 2019), https://blog.malwarebytes.com/security-world/privacy-security-world/2019/03/what-congress-means-when-it-talks-about-data-privacy-legislation/ [https://perma.cc/BB92-EKUR] (discussing how Congress reacted to the leaking of Supreme Court nominee, Robert Bork's video rental history by passing the Video Privacy Protection Act in the late 1980s).

[16] *Id.* (discussing recent public opinion and concerns regarding of data regulation made by 2020 presidential candidates).

[17] *Id.* (discussing proposals by Senators Klobuchar, Rubio, Wyden, and Schatz which would regulate data collection practices in various ways).

[18] *Id.* (describing the CCPA and mentioning several enforcement actions arising from GDPR).

[19] California Consumer Privacy Act of 2018, CAL CIV. CODE §§ 1798.100–1798.199 (West 2020).

these entities must give consumers the option to opt-out of data sales while still providing them with equal service.[20] Furthermore, upon request, these entities must give consumers a full report of the data collected from them and outline what these entities have done with that data.[21]

Other states like New York, Massachusetts, Maryland, Hawaii, and North Dakota have proposed state privacy legislation modeled after the CCPA and GDPR.[22] Furthermore, senators from Washington, Hawaii, Minnesota, and Massachusetts have all submitted federal privacy bills that would emulate many of the key components of the CCPA and GDPR.[23] As more and more legislation is proposed and passed, a few fundamental questions arise: what is the problem that these laws aim to fix, and is it worth it? Without adequately addressing these questions, the proposed legislation seems premature, unwise, and potentially counterproductive.

This Note evaluates the recent calls for increased regulation in the private collection of consumer and user data. This Note focuses on analyzing why there has been a sudden explosion advocating for such regulation and addresses the need for regulation through the following framework: (1) consumer harm; (2) consumer expectations; and (3) economic growth and innovation.[24]

Following this introduction, Part II of this Note briefly summarizes the background and current state of privacy laws within the U.S. Part III looks at the three reasons outlined above as to why the U.S. does not need increased regulation. Subsection A of Part III starts with the general proposition that regulation should seek to remedy a harm, and harms that are without significant societal or economic costs should not be remedied. The rest of subsection A attempts to show that

---

[20] *Id.*

[21] *Id.*

[22] Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), https://www.varonis.com/blog/us-privacy-laws/.

[23] Cameron Kerry, *Game on: What to Make of Senate Privacy Bills and Hearing*, BROOKINGS (Dec. 3, 2019), https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

[24] Many prominent academics have cautioned against privacy arguments regarding technology, however, much of their focus has been on Constitutional law. *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (cautioning that courts should not rush to adjust Fourth Amendment law to new technologies but should wait to see how those technologies play out before creating sweeping precedent).

the harms written of in the literature either do not rise to a sufficient level of societal or economic damage to warrant additional legislation or can be remedied through existing laws. Subsection B starts by examining the Privacy Paradox[25] and seeks to explain this paradox based on consumer expectations and agreements through contract law. Subsection C looks to the economic and innovation implications of enacting restrictive regulations by comparing the U.S. and the EU, as well as by looking at preliminary effects from recently implemented data protection laws. Part IV utilizes the conclusions of Part III and suggests possible solutions that do not include expansive regulation of data privacy. Lastly, Part V concludes the note.

II. Legal and Historical Background of Privacy and Data Collection Laws in the United States

Before making any conclusions about the validity and necessity of new comprehensive regulation, it is important to understand the current data regulatory system and how that system developed.

A. Privacy Rights in Tort and State Law

The idea of privacy rights allowing individuals to be free from invasions of privacy, or a "right to be let alone" first arose in the U.S. due to concerns associated with technological advances which facilitated public access to information—namely the increasing prevalence of photographs and newspapers in the latter part of the nineteenth century.[26] Spurred by the spread of such invasive technologies, in 1890, Samuel Warren and Louis Brandeis wrote *The Right to Privacy*, which argued for the evolution of the common law to protect this new "right to be let alone."[27] The Warren and Brandeis article is largely credited as the birth of the concept of a right to privacy in American

[25] Holland, *infra* note 147 at 893 (explaining that the Privacy Paradox refers to an inconsistency between consumer desires for protecting their personal data and contradictory consumer behaviors).

[26] George Ashenmacher, *Indignity: Redefining the Harm Caused by Data Breaches*, 51 WAKE FOREST L. REV. 1, 21 (2016) (discussing how Samuel Warren and Louis Brandeis's article, *The Right to Privacy*, was influenced by the increasing prevalence of photography, newspapers, and gossip press).

[27] *Id.*

law, and its influence slowly grew as the right to privacy trickled into the common law by gaining tacit acceptance in various courts.[28]

However, the distinct torts relating to privacy remained hazy and disorganized until seventy years later when Professor William Prosser undertook an expansive review of all caselaw that related to privacy and showed that the concepts of the right to be let alone had crystalized into four distinct privacy torts:

1. Intrusion upon the plaintiff's seclusion, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[29]

Today these torts are widely established at common law[30] and are recognized under the Restatement (Second) of Torts.[31] The future development of the common law use of these torts, specifically the tort of public disclosure of private facts and the tort of intrusion upon seclusion, could potentially lead to a wider protection of privacy for users who are harmed through the collection and dissemination of the data they generate.[32]

Under the disclosure of private facts tort, a bad actor who "gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reason-

---

[28] *Id.*

[29] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); *see* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 482–83 (2006).

[30] *See* McCall v. Courier-Journal and Louisville Times Co., 623 S.W.2d 882, 887 (Ky. 1982) (adopting the Restatement Second's four distinct privacy torts into Kentucky common law); Harris by Harris v. Easton Pub. Co., 483 A.2d 1377, 1383 (Pa. Super. Ct. 1984) (concluding that the Restatement Second "most ably defines the elements of invasion of privacy as that tort has developed in Pennsylvania.").

[31] RESTATEMENT (SECOND) OF TORTS § 652A (AM. LAW INST. 1977).

[32] Alexander H. Tran, Note, *The Internet of Things and Potential Remedies in Privacy Tort Law*, 50 COLUM. J.L. & SOC. PROBS. 264, 280 (2017) (advocating for the extension of the four privacy torts so that they can be widely used in technology related litigation).

able person, and (b) is not of legitimate concern to the public."[33] Courts have found parties liable under this tort for the public disclosure of a person's health status, financial information, and autopsy photographs.[34] The use of these torts to address wrongs that occur in the context of modern technology is relatively new and sparsely used,[35] but a relevant example occurred in the case of *Michaels v. Internet Entertainment Group, Inc.* where the plaintiff was able to rely on the private facts tort to secure a preliminary injunction to halt the online distribution of a personal sex tape.[36] The private facts tort could be expanded to protect against the dissemination of someone's internet searches and activities that pertain to sensitive, personal information. Additionally, with how much society utilizes devices and applications that collect user data on a variety of things, including exercise and eating habits, sleeping patterns, mental fitness, and driving patterns, this tort could become a useful tool in protecting these data from being disseminated to third parties and the public.[37]

For the tort of intrusion upon seclusion, one is liable if they intentionally "intrude[], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, … if the intrusion would be highly offensive to a reasonable person."[38] This tort would apply to an actor rummaging through someone's papers or personal effects, as well as if the actor were to observe a person in cir-

---

[33] RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

[34] Tran, *supra* note 32, at 285–86 (discussing a case where a plaintiff prevailed when their AIDS diagnosis was broadcast by a TV station and another case where a plaintiff prevailed when the details of their child support arrangement was published by a tabloid).

[35] Adam Thierer, *The Pursuit of Privacy in a World Where Information Control Is Failing*, 36 HARV. J.L. & PUB. POL'Y 409, 451–53 (2013) (acknowledging the development of privacy torts and the prominence of privacy class actions whenever data breaches occur); Tran, *supra* note 32, at 264 (discussing notable cases where courts have applied the tort of public disclosure of private facts); *but see* Neil M. Richards et al., *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1888, 1889 (2010) (explaining the general ineffectiveness of these torts in regards to the collection and dissemination of personal user data).

[36] Michaels v. Internet Entm't Grp., Inc., 5 F. Supp. 2d 823, 839 (C.D. Cal. 1998).

[37] Tran, *supra* note 32, at 289.

[38] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

cumstances where that person would reasonably expect solitude.[39] This tort is especially promising in the data collection context for two reasons. First, it does not rely on the dissemination of information, but only the collection of information.[40] Second, it does not depend on the content of the information being gathered, but only that the information was collected in a manner intrusive to a reasonable person's expectation of seclusion.[41] Taken together, these points could allow this tort to police a website or ISP's collection of data, even mundane data, if the method of collection is unscrupulous. These privacy torts remain a viable tool in the policing of modern data collection and further development and expansion could lead to a system with robust user protections.

In addition to state common law actions, every state has its own different set of relevant consumer privacy laws.[42] Some states focus on transparency from data collectors, while other states may omit this altogether.[43] The only common denominator in the amalgam of state privacy laws is that all states have some sort of notification requirement for data breaches.[44] However, even within the category of laws requiring data breach notifications, how a business must notify consumers and what they must notify them of varies greatly by state.[45] Because of the breadth and variability of state law, a full summary is outside of the scope of this Note and an outline of the federal framework on data privacy will be more relevant.

---

[39] Tran, *supra* note 32, at 290–97 (discussing various acts that constitute the intrusion upon seclusion privacy tort).

[40] *Id.* at 295 (quoting Professor Neil Richards' suggestion that the intrusion tort seeks to prevent "'unwanted collections or accumulations of information rather than preventing the dissemination of already-collected information.'").

[41] *Id.* at 291 ("Additionally, the intrusion must be by invasion into a place in which the plaintiff has secluded himself.").

[42] Noah Ramirez, *The Great Big List of Data Privacy Laws by State*, OSANO (June 2, 2020), https://www.osano.com/articles/data-privacy-laws-by-state [https://perma.cc/2KHY-QU8Z] (discussing various states' data privacy laws).

[43] STEPHEN P. MULLIGAN ET AL., CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 54 (2019) ("[S]ome state laws focus solely on data security or address a particular security concern, such as data breach notifications.").

[44] Ramirez, *supra* note 42.

[45] *Id.*

B. Federal Legislation: A Piecemeal Approach

In creating a federal framework, Congress has taken a reactive, rather than proactive, approach to legislating privacy rights—waiting until a well-publicized harm arises before legislating.[46] This has led to a piecemeal approach, where very specific categories of privacy are regulated and strictly protected.[47] So far, the regulations protect:

- Consumer Credit Reports
- Electronic Communications
- Federal Agency Records
- Education Records
- Bank Records
- Cable Subscriber Information
- Video Rental Records
- Motor Vehicle Records
- Health Information
- Telecommunications Subscriber Information
- Children's Online Information
- Consumer Financial Information[48]

---

[46] Ruiz, *supra* note 15 (quoting Michelle Richardson, director of the data and privacy project at the Center for Democracy and Technology, "[t]his reactive approach is just how Congress works. This country has generally allowed companies to do their thing until something goes quite wrong ….").

[47] Devin W. Ness, *Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It*, 31 CARDOZO ARTS & ENT. L. J. 925, 944 (2013) ("The United States has to date taken a piecemeal approach to information privacy law, resulting in "[a] patchwork of federal and state laws … to protect the privacy of certain personal information" rather than serving as a 'comprehensive federal privacy statute that protects personal information held by both the public sector and the private sector.'").

[48] *Id.* (citing the: Fair Credit Reporting Act; Electronic Communications Privacy Act of 1986; Privacy Act of 1974; Family Educational Rights and Privacy Act of 1974; Right to Financial Privacy Act of 1978; Cable Communications Policy Act of 1984; Video Privacy Protection Act of 1988; Driver's Privacy Protection Act of 1994; Health Insurance Portability and Accountability Act of 1996; Communications Act of 1934; Children's Online Privacy Protection Act of 1998; Consumer Financial Protection Act of 2010).

These laws address the need to protect "sensitive data, more vulnerable individuals, but also harm to consumers and fraud, which is at the heart of many concerns about privacy data and data protection …."[49] Even still, the piecemeal system leaves some surprising categories unprotected; for example, a person's web browsing history, photographs and videos posted on social media, and physical location data would not fall under federal regulation.[50] However, even if something is outside of a protected category, it is still subject to the Federal Trade Commission's (FTC) oversight under its expansive powers from Section 5 of the Federal Trade Commission Act (Section 5), industry self-regulation, and more recently, the Consumer Financial Protection Bureau (CFPB). [51]

C. FTC Section 5, Self-Regulation, and the CFPB

The Federal Trade Commission Act was enacted in 1914, with the goal of enforcing antitrust law by preventing unfair methods of competition.[52] In 1938, the Wheeler-Lea amendment to Section 5 was passed.[53] This expanded the FTC's authority from policing competetion into the sphere of consumer protection.[54] Section 5 reads in part "[t]he [FTC] is hereby empowered and directed to prevent persons, partnerships, and corporations … from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or

---

[49] Jennifer Huddleston, *Preserving Permissionless Innovation in Federal Data Privacy Policy*, 22 J. INTERNET L. 17, 18 (2019).

[50] Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/#_ftn53 [https://perma.cc/X9TC-24CY] (explaining how the company, InMobi, circumvented protections to track consumer's location without consent).

[51] Rebecca Lipman, *Online Privacy and the Invisible Market for our Data*, 120 PENN ST. L. REV. 777, 787–90 (2016) ("The FTC has authority from § 5 of the Federal Trade Commission Act to prohibit 'unfair or deceptive acts or practices.'").

[52] MULLIGAN, *supra* note 43, at 30 (explaining the history of the FTC Act).

[53] *Id.* ("While the FTC Act was originally enacted in 1914 to strengthen competition law, the 1938 Wheeler-Lea amendment revised Section 5 of the Act to prohibit a broad range of unscrupulous or misleading practices harmful to consumers.").

[54] *Id.* ("The Act gives the FTC jurisdiction over most individuals and entities, although there are several exemptions.").

practices in or affecting commerce." [55] The undefined, broad reference to "unfair acts" was a deliberate point by Congress to ensure the adaptability of Section 5 to future problems, resulting in its ability to enforce modern data privacy concerns. [56]

Under the broad statutory power of Section 5, the FTC has the authority to police a company's data collection and use, provided that said company deviated from its privacy policy provided to users.[57] For example, the FTC found Snapchat to be engaging in deceptive practices when it failed to adhere to the practices laid out in their privacy and security policies.[58] Similar enforcement actions have been brought by the FTC against Google, Facebook, and Myspace.[59] Further, Section 5 has also been used to ensure that companies protect user data by not subjecting it to unreasonable risk.[60]

It is important to note that Section 5 was not written with data privacy concerns in mind; it applies to practices within all industries, with the exception of banks and common carriers.[61] In reality, the application of Section 5 to privacy in data privacy may be hindered by the definition of "unfair" practices. Specifically, Congress has codified "unfair" to mean a practice that "(1) causes or is likely to cause substantial injury to consumers which is (2) not reasonably avoidable by consumers themselves and (3) not outweighed by countervailing benefits to consumers or to competition."[62] This standard usually requires: (1) a showing of substantial injury, usually proved through significant monetary harm; (2) a showing that there was "behavior that unreason-

---

[55] 15. U.S.C. § 45(a)(2) (2016).

[56] Ashenmacher, *supra* note 26, at 45–46 (explaining Congress's purpose in enacting the FTC Act and subsequent Wheeler-Lea Amendment).

[57] Lipman, *supra* note 51, at 790 (highlighting actions the FTC took against Facebook and Snapchat for misleading users on how their data was to be used).

[58] Ashenmacher, *supra* note 26, at 45 n.285 (quoting the FTC's Complaint against Snapchat to explain the legal foundation underlying the deceptive practices charge).

[59] Thierer, *supra* note 35, at 449–52 (summarizing enforcement actions brought against Facebook and Google as well as noting FTC charges against Myspace).

[60] *Id.* (explaining the FTC's effort to protect users' data by bringing actions when companies fail to maintain reasonable data security).

[61] 15 U.S.C. § 45(a)(2) ("The [FTC] is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions, … Federal credit unions … , common carriers …").

[62] 15 U.S.C. § 45(n) (2016).

ably creates or takes advantage of an obstacle to the free exercise of consumer decision making;" and (3) a showing that the injury is not outweighed by consumer or competitive benefits from the practice.[63]

While the standards for "unfair" practices are quite high, the FTC has been able to rely on the "deceptive" practices language in bringing hundreds of enforcement actions.[64] It is important to note that these enforcement actions almost always lead to settlement or consent decrees between the FTC and the implicated companies.[65] So, while there are few meaningful judicial decisions regarding deceptive and unfair policies, in practice, the settlements function as a kind of common law that guides companies on appropriate data practices.[66]

The FTC defines a "deceptive" practice as a material "representation, omission, or practice that is likely to mislead [a] consumer" who is "acting reasonably in the circumstances."[67] In the data privacy context, rulings on deceptive practices are almost always based on whether a company has adhered to its own privacy policies.[68] By breaking a specific promise to consumers, a company has engaged in deceptive practices and is subject to enforcement actions by the FTC.[69] However, recently it has become common practice for companies to skirt around the "deceptive" practices language by making their privacy or security agreements overly inclusive or vague.[70] An intrusive data collection practice that is openly announced is not a violation of Section 5.[71] To combat this, the FTC can enact new rules broadening the scope of unfair and deceptive practices, thus preventing

---

[63] Ashenmacher, *supra* note 26, at 45–47.

[64] MULLIGAN, *supra* note 43, at 32 ("The FTC has brought hundreds of enforcement actions against companies alleging deceptive or unfair data protection practices.").

[65] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 606 (2014).

[66] *Id.* at 619–26.

[67] MULLIGAN, *supra* note 43, at 31.

[68] *Id.* at 32 ("The FTC has taken the position that companies act deceptively when they gather, use, or disclose personal information in a way that contradicts their posted privacy policy or other statements, or when they fail to adequately protect personal information from unauthorized access despite promises that that they would do so.").

[69] *Id.*

[70] Lipman, *supra* note 51, at 790 (illustrating how Groupon was very transparent in their privacy policy that they planned to share users' location data, allowing them to avoid FTC action).

[71] *Id.*

specific practices like overinclusive privacy policies.[72] So despite these limitations, Section 5 still leaves in place the ability and authority for the FTC to address aspects of consumer privacy concerns in the field of technology.

Outside of its Section 5 capacity, the FTC has endorsed the idea of self-regulation since the late 1990s.[73] It has largely operated under the belief that "self-regulation is the least intrusive and most efficient means to ensure fair information practices, given the rapidly evolving nature of the Internet and computer technology."[74] More recently, the FTC has released its guidelines for self-regulation, entitled *Self-Regulatory Principles for Online Behavioral Advertising* (FTC Guidelines).[75] The FTC Guidelines provide industry guidance that many companies have adopted as best practices.[76] Included is an emphasis on "four key principles: Transparency and Consumer Control, Reasonable Security and Limited Data Retention, Affirmative Express Consent for Material Changes, and Affirmative Express Consent to Using Sensitive Data for Behavioral Advertising."[77] Under these principles, website operators are encouraged to inform users of data collection practices upon entering the website, and to provide users with the ability to opt-out of data collection.[78] While the FTC Guide-

---

[72] *But see* MULLIGAN, *supra* note 43, at 31–32 nn.300–02 (acknowledging that while the FTC has the power to make "trade regulation rules," it must meet numerous additional requirements outside of the usual notice-and-comment procedures in the Administrative Procedure Act, which results in the FTC rarely enacting new trade regulation rules).

[73] Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation*, 34 SEATTLE U. L. REV. 439, 459 (2011) (discussing the FTC's adoption of self-regulation).

[74] MARTHA K. LANDESBERG & LAURA MAZZARELLA, FED. TRADE COMM'N., SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 6 (1999).

[75] FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009).

[76] Shawn M. Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299, 307 (2018) (describing the guidelines and best practices issued by the FTC).

[77] Benjamin R. Mulcahy & Dante M. DiPasquale, *Efficiency v. Privacy: Is Online Behavioral Advertising Capable of Self-Regulation*, 15 No. 4 CYBERSPACE LAW. 16 (2010).

[78] Ieuan Jolly, *Data Protection in the United States: Overview*, THOMPSON REUTERS PRACTICAL L. (July 1, 2016), https://content.next.westlaw.com/6-502-0467?transitionType=Default&contextData= (explaining how a host of major pieces of federal legislation include provisions giving consumers the

lines are purely optional, most digital advertising companies belong to the Network Advertising Initiative, which has adopted the FTC Guidelines and can impose general sanctions as well as suspend or revoke memberships for noncompliance.[79] Moreover, the FTC has imposed third-party self-regulatory agreements through consent decrees, such as requiring Facebook to monitor independent app developers for privacy violations.[80]

And lastly, while a relatively new organization, the CFPB has strong regulatory authority regarding privacy in parts of the technology industry.[81] The CFPB was created to enforce federal consumer financial laws and to regulate consumer financial products.[82] The CFPB has broad rulemaking, supervisory, and enforcement authority over "covered persons,"[83] which is defined as "any person that engages in offering or providing a consumer financial product or service" and any affiliate that acts as a service provider to such person.[84] This allows the CFPB to exercise jurisdiction over almost all financial technology companies that offer consumer products.[85] Importantly, as more traditionally non-financial technology companies like Apple, Amazon, and Facebook have begun to create their own payment systems, the CFPB has the rulemaking authority to bring these companies within their jurisdiction.[86] In enforcing consumer financial laws, the CFPB has the authority to ensure that consumers have effective control over their

---

right to opt out if they do not want their information shared with certain third parties).

[79] Boyne, *supra* note 76, at 306–07 (stating that the National Advertising Initiative may "impose sanctions, including suspension or revocation of membership and may refer the matter to the Federal Trade Commission for noncompliance.").

[80] *See* Rory Van Loo, *The New Gatekeepers: Private Firms as Public Enforcers*, 106 VA. L. REV. 467, 467 (2020).

[81] Rory Van Loo, *Technology Regulation by Default: Platforms, Privacy, and the CFPB*, 2 GEO. L. TECH. REV. 531, 532 (2018).

[82] 12. U.S.C. § 5511(a) (2016).

[83] 12. U.S.C. § 5511(c)(4) (2016).

[84] 12. U.S.C. § 5481(6) (2016).

[85] *See* Van Loo, *supra* note 81 at 532–44 (discussing the CFPB's enforcement actions over PayPal and Dwolla, as well as how the CFPB sets guidelines for private data sharing between banks and fintech platforms like Mint and Credit Karma).

[86] It should be noted that the CFPB's jurisdiction over a traditional technology company that adds a financial product would be limited to the financial parts of that company's platform. *Id.* at 544.

financial data and to ensure that companies are adequately protecting such data.[87] In the latter respect, the CFPB has quickly emerged a leading agency, bringing it alongside the FTC.[88] So, while the FTC has been the traditional go-to agency regarding consumer privacy, the arrival of the CFPB in this area of regulation should be closely monitored as it continues to explore the contours of its powers going forward.[89]

To summarize, targeted federal laws, FTC and CFPB regulation represent the general piecemeal approach that governs most of this country. This piecemeal system presents drawbacks in that many of the targeted statutes have not been updated to reflect changes in current technologies and may not have privacy as their primary purpose, thus making the privacy sections of the law difficult to comprehend and easily circumventable.[90] Furthermore, the very fact that they are disjointed makes it difficult to find the relevant privacy laws, determine how those different laws interact, and taken together, identify what those laws require for compliance.[91] However, this piecemeal approach allows for "a diverse range of data usage and [a] diverse array of privacy options for consumers while still providing a means of redress when harm does occur" and remains "flexible and adaptive to changes that may occur."[92]

III. Cautioning Against Additional Regulation

As mentioned earlier, there have been recent pushes for increased privacy regulation on the collection and dissemination of consumer data.[93] There are several reasons given in the literature as to why additional regulation is needed. First, many people believe

---

[87] *Id.* at 533–34.
[88] *Id.*
[89] *Id.* at 544–45 (noting the possibility of a future clash regarding the intersection of jurisdiction between the CFPB and the FTC in policing companies' data-security practices).
[90] Ness, *supra* note 47, at 945–51 (highlighting the issues with the Electronic Communications Privacy Act and the Health Insurance Portability and Accountability Act as examples of the difficulties in navigating the different statutes that comprise the privacy laws in the United States).
[91] *Id.* (describing the "patchwork" of laws that create the privacy legal framework in the United States).
[92] Huddleston *supra* note 49, at 18.
[93] *See, e.g.*, Ruiz, *supra* note 15 (describing mounting public support for data protection in light of the recent Equifax and Cambridge Analytica scandals).

privacy to be a fundamental, inalienable right.[94] This belief may stem from the Supreme Court's holdings on the existence of a substantive right to privacy, explicit declarations in state constitutions, or the EU's Charter of Fundamental Rights.[95] Second, there is a feeling of general unease amongst people when confronted with the fact that large corporations hold vast amounts of data on most of the population.[96] Third, consumers are concerned that because of a lack of transparency, they are unable to fully comprehend the extent of their agreements when consenting to provide data.[97] These examples represent a few of the most compelling reasons driving much of the discussion regarding the need for increasing regulation; however, they may not represent the full picture.

In researching this topic, three specific areas are particularly persuasive in cautioning against the push for regulation: (1) outside of areas protected by existing federal law, there seems to be no significant harms generated by the free, consensual collection and dissemination of user data; (2) consumers seem willing to trade their personal data in return for using these services; and (3) the current regime of self-

---

[94] Aaron Shubert, *Not All Those Who Wander Are Lost: The Pathway Towards American Data Privacy Law*, 48 HOFSTRA L. REV. 835, 864 (2020) (explaining that a major reason why California passed the CCPA was due to the fact that privacy was added to the list of inalienable rights in the California Constitution).

[95] *Id.* at 836 ("Landmark [Supreme Court] cases that demonstrate this perceived right to privacy include *Griswold v. Connecticut*, *Roe v. Wade*, and *Lawrence v. Texas*, to name a few."); *but see* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727 (2020) (clarifying that the Bill of Rights consists of negative rights against the state and that few constitutional rights apply to private actors, much less creating a right to data protection).

[96] Hartzog & Richards, *supra* note 95, at 1709–10 (highlighting how people have "grown wearier and more skeptical of digital tech, and social media in particular."); *see* Marissa Merrill, Comment, *An Uneasy Love Triangle Between Alexa, Your Personal Life, and Data Security: Exploring Privacy in the Digital New Age*, 71 MERCER L. REV. 637, 638–42 (2020) (summarizing survey data that reported respondents' general unease towards the 'creepy' nature of Amazon Alexa devices' constant listening and recording).

[97] Joanna Kessler, Note, *Data Protection in the Wake of the GDPR: California's Solution for Protecting "The World's Most Valuable Resource,"* 93 S. CAL. L. REV. 99, 100–03 (2019) (arguing that because most consumers are unaware of the high value of data, mixed with the complex nature of privacy agreements, they are unable to make informed economic determinations when agreeing to exchange data for free services).

regulation promotes innovation and growth in one of America's most valuable industries.

A. Where Is the Harm?

The first reason to be cautious of expanding regulation in commercial data collection and dissemination is that the regulation might not be addressing any significant harms. Consumer protection regulation should seek to either address or prevent significant consumer harm.[98] So, the question at hand is: what is the harm to consumers, and if there is harm, is it significant enough to warrant regulation?

Defining the harm resulting from breaches of privacy has long been problematic, as privacy itself is an amorphous, hard-to-define concept; "nobody seems to have any very clear idea what it [privacy] is."[99] Not only is privacy difficult to define, but it also protects a dizzying array of interests, spanning from safeguarding personally identifiable information to a constitutional right to privacy inferred from the many "penumbras" of the Bill of Rights.[100] Despite privacy's amorphous nature and the breadth of categories it covers, there have been many attempts to describe and categorize the harms stemming from invasions of privacy.[101] The most cogent of these attempts divides privacy harms into two categories: subjective and objective privacy harms[102]

---

[98] Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, 23 COMMLAW CONSPECTUS, 1, 4 (2014) ("Our consumer protection laws encourage us to focus on consumer harm, whether the cause of the harm is deception or unfairness.").

[99] Solove, *supra* note 29, at 480 (quoting philosopher Judith Jarvis Thomson, Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 272 (Ferdinand David Schoeman ed., 1984)).

[100] Griswold v. Connecticut, 381 U.S. 479, 484–86 (1965) ("The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.").

[101] Ashenmacher, *supra* note 26, at 6 (highlighting an attempt by Professors Daniel Solove and Woodrow Hartzog to define the harms stemming from privacy invasions).

[102] Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1131–32 (2011) (outlining the objective and subjective categories of privacy harm).

Subjective privacy harms can be thought of as one's perception of unwanted observation and its accompanying mental states.[103] The instinctive feelings of fear, anxiety, and creepiness that arise whenever privacy is violated become the harms themselves.[104] Examples of this include: the anxiety experienced by individuals affected by data breaches, the chilling effect on speech once one is aware they are being watched,[105] and the emotional injury tenants suffered after a landlord planted listening devices in their bedroom.[106]

Once these subjective harms are highlighted, the call to recognize and stop invasions of privacy becomes significantly easier and follows an almost elementary formula: "Imagine invasions of your privacy, the argument runs. Do they not seem like violations of your very personhood? Since violations of privacy seem intuitively horrible to everybody, the argument continues, safeguarding privacy must be a legal imperative, just as safeguarding property or contract is a legal imperative."[107] When confronted with subjective privacy harms, it is this line of reasoning that takes over and drives the "need" for regulation.

In the specific context of technology companies gathering user data for Behavioral Advertising, the "harms" become more speculative and less cognizable.[108] If the harms from violations of privacy are distilled down to subjecting people to feelings of uneasiness and creepiness, the question remains as to whether this is something that

---

[103] *Id.* ("Examples of subjective privacy harms include everything from a landlord eavesdropping on his tenants to generalized government surveillance.").

[104] Solove, *supra* note 29, at 480 ("What commentators often fail to do, however, is translate those instincts into a reasoned, well-articulated account of why privacy problems are harmful.").

[105] Laird v. Tatum, 408 U.S. 1 (1972) (holding that plaintiffs failed to present a justiciable controversy in complaining that Army surveillance of lawful civilian political activity produced a chilling effect on their First Amendment rights).

[106] Hamberger v. Eastman, 206 A.2d 239 (N.H. 1964) (holding that a landlord's instillation of a listening and recording device without plaintiff's knowledge violated their right to privacy).

[107] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1153, 1154 (2004).

[108] Thomas M. Lenard & Paul H. Rubin, *Big Data, Privacy and the Familiar Solutions*, 11 J.L. ECON. & POL'Y 1, 25, 26 (2015) ("Discussions of harm in the literature are largely speculative and hypothetical ….").

warrants protection from the law.[109] The issue with such a standard becoming legally cognizable is that it is subjective and necessarily protean.[110] At best, one could come up with some sort of reasonable person standard, but the amount of creepiness that would offend the reasonable person is hardly anything close to an objective measure.[111] This standard would then need to somehow be weighed in cost-benefit analyses to guide policy.[112] Furthermore, most new technologies will initially be met with feelings of creepiness, and society will either adapt and normalize those technologies, or they will be rejected by the market.[113] For example, as mentioned earlier, the inspiration that birthed the original call for a right to privacy was Samuel Warren and Louis Brandeis's fears over the increasing prevalence of photography, newspapers, and gossip press.[114] While perhaps the reasonable person in 1890 would find their privacy offended by photographs, hardly anyone thinks twice about such things today. If society had shunned those groundbreaking developments to protect against the harms of creepiness, who knows what the cost would have been to the scientific and social advancement of society.

There is, however, a specific type of subjective privacy harm —injury to personal dignity—which garners significant discussion in

---

[109] Thierer *supra* note 35, at 418 ("But why should 'creepiness' be the standard by which policymakers judge privacy harms at all?").

[110] *Id.* at 417–21 (highlighting the various issues in adopting creepiness as the standard for privacy harms).

[111] *Id.* (arguing that "'[c]reepiness' is simply too open-ended and subjective ….").

[112] *Id.* (explaining how "creepiness" operates as an "amorphous standard for policy analysis or legal and regulatory action [that] leaves much to the imagination and opens the door to creative theories of harm that may not actually represent true harm at all and could be exploited by those who ignore the complex tradeoffs at work.").

[113] *Id.* at 420 (illustrating how the launch of Gmail was initially marred by claims of privacy violations, but has since become the premier email service, as users "adapted their privacy expectations to accommodate this new service, which offered them clear benefits (free service, generous storage, and improved search functionality) in exchange for tolerating some targeted advertising.").

[114] Ashenmacher, *supra* note 26, at 21 (discussing how Warren and Brandeis emphasized instantaneous photographs, newspaper enterprise, and the gossip press as new technology encroaching on privacy).

the literature and deserves a brief discussion.[115] Dignity and its close counterpart, honor, have had long and storied traditions in European law.[116] However, there are fundamental tensions between safeguarding dignity and the more American value of liberty, specifically, liberty against the state.[117] Nowhere is the diametric opposition of these concepts more evident than in the protections of free speech.[118] So, while Europeans afford protections against simple disrespect and hateful speech through the law of "insult," as an extension of protecting honor and dignity,[119] American jurisprudence vehemently protects the liberty of free speech, including hate speech.[120] And while there have been notable attempts to introduce dignity to American law, such as Justice Kennedy's opinion in *Lawrence v. Texas*, the overarching American trend in privacy still favors liberty over dignity.[121] Even though Europeans have found a way for more robust protections of personal privacy, their ability to do so may be rooted in their capacity to protect against harms to dignity, a means that is not necessarily available in the American legal system.

The second category of harm, objective privacy harms, can best be described as "harms that are external to the victim and involve

---

[115] Whitman, *supra* note 107, at 1161 ("Continental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*.").

[116] *Id.* at 1164–68 (discussing European traditions of dignity and their protections in European law).

[117] *Id.* at 1161 ("By contrast [to Europe], America, in this as in so many things, is much more oriented toward values of liberty, and especially liberty against the state.").

[118] *Id.* at 1171 ("Indeed, the history of continental privacy law has been, in essence, the history of the resistance, in the name of "honor," to two of the fundamental values of American liberty: the value of free speech, and the value of private property as distributed through the market.").

[119] *Id*. at 1164 ("Everybody is protected against disrespect, through the continental law of 'insult,' a very old body of law that protects the individual right to "personal honor.").

[120] Matal v. Tam, 137 S. Ct. 1744, 1764 (2017) ("Speech that demeans on the basis of race, ethnicity, gender, religion, age, disability, or any similar ground is hateful; but the proudest boast of our free speech jurisprudence is that we protect the freedom to express 'the thought we hate.'").

[121] Whitman, *supra* note 107, at 1162 (discussing *Lawrence v. Texas* as the notable deviation from the trend of American law featuring liberty over dignity); *see also* Obergefell v. Hodges, 576 U.S. 644, 663 (2015) ("In addition these liberties [liberties protected by the Due Process Clause of the Fourteenth Amendment] extend to certain personal choices central to individual dignity and autonomy ….").

the forced or unanticipated use of personal information."[122] Examples of this include: identity theft, negative judgement by peers formed from gossip, seizing a drunk driving suspect's blood, and getting placed on a No Fly List.[123] It is important to note that in all of these examples, the personal information of the victim is used against them by an external force without their consent.

However, "[i]t is not a privacy harm to use a person's information if he himself publicized it or if he understood and agreed to the use."[124] Because of this consent requirement, very few objective privacy harms fall within the realm of technology companies' collection and dissemination of user data.[125] The major harms in this category include identity theft, reputational damage, and impacts on credit; all of which are currently regulated, or could be remedied through the existing federal privacy law framework or by common law actions.[126] For example, if someone's internet searches are revealed to the public, causing damage to their reputation, they can sue under the common law tort of disclosure of embarrassing facts.[127] If a data breach occurs and a person's health information is released and their identity is stolen, HIPPA provides for breach notifications and civil enforcement.[128] And generally, most states have private rights of action available against the perpetrator of identity theft.[129]

---

[122] Calo, *supra* note 102, at 1148.

[123] *Id.* at 1147–52.

[124] *Id.* at 1148, 1150 (discussing that liberal economics generally stands for the principle that "free and anticipated uses of personal information do not constitute privacy harms and must remain unregulated.").

[125] Lenard & Rubin, *supra* note 108, at 26 ("Some examples of what have been described as 'objective privacy harms' include: use of blood test data for drunk driving; data used for a no-fly list; and police use of information from a psychologist. Only some of these are related to big data, but more importantly, none involve commercial information.").

[126] Ness, *supra* note 47, at 944 (describing Congress's "piecemeal approach" to privacy law resulting in a "patchwork of federal and state laws" rather than a comprehensive all-inclusive piece of legislation.).

[127] Tran, *supra* note 32, at 265 ("[T]his Note argues that the common law, specifically privacy torts, provides a partial remedy for individual consumer harms … In particular, the 'disclosure of private facts' and 'intrusion upon seclusion' torts are suitable vehicles to regulate the IoT.").

[128] MULLIGAN, *supra* note 43, at 10–11 (discussing HIPAA's privacy regulations of protected health information).

[129] CAL CIV. CODE § 1798.93 (West 2020) (creating a private right of action for identity theft).

Because objective privacy harms likely fall within federally protected categories for sensitive data like financial records, credit scores, and health records, those harms are addressed,[130] and what remains are subjective privacy harms. These harms consist of vague feelings of uneasiness and creepiness that are internalized to the victim and unquantifiable. Whether this is a significant enough harm to warrant regulation should ultimately be decided through informed policy debate. But it should be clear that in weighing the costs and benefits of regulation, the harm that regulators are addressing is one based entirely upon subjective feelings.

B. Free Services for Data

The second reason to be wary of additional regulation is that many consumers are willing, and possibly even wanting to give up their data. Most online services are free, in the sense that consumers do not directly pay any money to use them.[131] Instead, consumers indirectly pay for these online services by allowing the site to collect and disseminate information gathered from the consumer while using these services.[132] For example, imagine a consumer visits a website looking for airline flights to New York.[133] They then go on a newspaper site to read about the Washington Nationals baseball team, and while on that site, they get ads for flights from Washington D.C. to New York.[134] In this scenario the user agreed to the use of cookies by both websites, and both websites belonged to an advertising network, where the network paid the websites to place cookies on their user's browsers.[135] This is the traditional way that Behavioral Advertising works and how consumers end up "paying" websites that do not utilize a paywall. New and proposed regulation may dismantle this free service-for-data model.

---

[130] Ness, *supra* note 47, at 944.
[131] Rosenberg, *supra* note 3 ("What many don't think about day-to-day, however, is that all of these services are free.").
[132] *Id.* ("AdWords advertisements integration touches almost all of Google's web properties. Any recommended websites you see when logged in to Gmail, YouTube, Google Maps, and other Google sites are generated through the AdWords platform.").
[133] Berger, *supra* note 5, at 6–9 (discussing DC to NYC airline web search example).
[134] *Id.*
[135] *Id.*

Traditionally, the main principles in many of the federal privacy laws and the FTC's guidance has emphasized a system of consent and disclosure, where data collecting firms should notify consumers that they are gathering their data and of what they plan to use the collected data for.[136] Recently the consent and disclosure framework has been expanded by the CCPA with the right of consumers to opt out of having their data sold to third parties.[137] The GDPR takes an even more extreme approach and creates a "privacy by default" structure where prior consent must first be obtained before data can be collected.[138] It has now become standard procedure for most websites to require users to accept terms of use, including the privacy terms, as well as allow some sort of opt-out to selling user data.[139] Dismantling this structure by encouraging opt-outs to data sales and cookie tracking may force these companies to provide lesser services or charge for services, both results that many consumers are unwilling to accept.[140] Thus, a large part of the privacy debate comes down to the question of whether or not consumers value their privacy over the services they access, and if not, should the law respect their decisions or are consumers in this space not to be trusted?[141]

---

[136] Strandburg, *supra* note 4, at 143 ("United States law and regulation have (at least this far) emphasized the notice and choice principles, with the results that, in the commercial data collection arena, the primary mechanism for implementing FIPs has been to have consumers agree to a businesses' data practices.").

[137] ROPES & GRAY, GDPR vs CCPA, (2019) (Powerpoint), https://www.ropesgray.com/-/media/Files/Prax-Pages/CCPA/GDPR-vs-CCPA.pdf [https://perma.cc/8JPJ-TZWA] (illustrating differences between the two regulations).

[138] CCPA vs GDPR | Compliance with Cookiebot, COOKIEBOT (May 28, 2020), https://www.cookiebot.com/en/ccpa-vs-gdpr/ ("The GDPR is focused on creating a 'privacy by default' legal framework for the entire EU, whereas the CCPA is about creating transparency in California's huge data economy and rights to its consumers.").

[139] *Id*. ("[T]he right to opt-out (CCPA) is best likened to the right to withdraw consent (GDPR) ….").

[140] *See* Daniel Castro, *National Survey Finds Few American Willing to Pay for Privacy*, CENTER FOR DATA INNOVATION (Jan. 16, 2019), https://www.datainnovation.org/2019/01/national-survey-finds-few-americans-willing-to-pay-for-privacy/ [https://perma.cc/259C-7QK9] (discussing a survey showing that only 25 percent of respondents were willing to pay for currently free online services if it meant less data collection).

[141] Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1894 (2013) (examining the need to strike

The legal basis governing the relationship between consumers and their access to free technology services is contract law.[142] A consumer must usually accept a website's terms of service and privacy policy before being able to use the website's services, which forms the basis of the contractual relationship.[143] In general, contracts enforce the reasonable expectations of parties[144] and should operate no differently when contracts take the form of terms of service and privacy agreements.[145] If consumers are willing to contract away parts of their privacy for the use of services, they should be allowed to do so. Even if the decision to give up privacy is a bad one, contract law respects these decisions, as not every contract is perfect, and most contracts will have a winner and a loser.[146]

To be sure, there are salient criticisms with contracts of adhesion that govern user privacy: consumers do not read the contracts; the contracts are not truly bargained for; the contracts are standardized; and consumers would not understand the contracts even if they read them.[147] At the core of these criticisms is that consumers lack information about the true extent to which their data is being used, and lack of awareness is to blame.[148] It is no surprise that nobody actually reads

---

a balance in privacy regulation between allowing people to consent and maximizing consumer protection through paternalistic regulation).

[142] Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 285 (2016) (describing how most internet privacy policies and terms of service agreements are generally treated as contracts of adhesion).

[143] *Id.* ("These [terms of service and privacy policy] agreements are contracts that practically every Internet user must accept for each website that she uses.").

[144] Nancy S. Kim & D.A. Jeremy Telman, *Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent*, 80 MO. L. REV. 723, 766 (2015) ("Contract law's primary objective is to enforce the reasonable expectations of the parties ….").

[145] *See* Kesan et al., *supra* note 142, at 285–86 (explaining that though online agreements are usually contracts of adhesion, they are still enforceable).

[146] Solove, *supra* note 141, at 1897 ("Contract law does not second-guess every agreement, even lopsided ones where one party did not fare very well.").

[147] H. Brian Holland, *Privacy Paradox 2.0*, 19 WIDENER L.J. 893, 907–908 (2010) (positing that online contracting for personal information does not involve any individualized, bargained-for agreements and that consumers do even not bother to read the contract language).

[148] Shara Monteleone, *Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behaviour-Aware Regulation*, 43

these agreements before accepting them, nor is it surprising that even had consumers read such agreements, they would only have a vague understanding of what they were contractually agreeing to.[149] However, these issues are not unique to privacy agreements for technology companies, as they have universally been documented and accepted as a problem with all consumer contracts, especially contracts of adhesion.[150] Perhaps a fundamental change to the law of contracts is needed regarding consumer contracts in general,[151] but that is beyond the scope of this Note. What can be said is that consumers generally believe they are agreeing to more privacy-invasive policies than what is actually being agreed to.[152] Outside the bounds of contract law, consumers may find protection from unscrupulous or invasive terms contained in privacy agreements through the FTC's Section 5 powers.[153] In 2009, the FTC found that Sears was engaging in deceptive practices when its software tracked consumers' total online

---

SYRACUSE J. INT'L L. & COM. 69, 75 (2015) ("Current privacy notices are ignored as they are often written in a not clear and easy language. In brief, they are hardly ever read by users and—even if read—very difficult to understand.").

[149] Solove, *supra* note 141, at 1884–85 (discussing the widely established phenomenon where the vast majority of users fail to read privacy policies before accepting them and the general difficulty for laypersons in comprehending said policies).

[150] Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173, 1225–30 (1983) (highlighting the issues with consumer contracts of adhesion).

[151] *But see* RESTATEMENT (SECOND) OF CONTRACTS § 211, cmt. a (AM. LAW INST. 1981) ("Standardization of agreements … are essential to a system of mass production and distribution.").

[152] *See* Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J.L. STUD. 69, 87 (2016) ("The key lesson from both the Facebook and e-mail data is that users of e-mail and social networking sites appear to regard even highly ambiguous privacy policy language as authorizing controversial company practices that implicate their personal privacy. Wilkinson-Ryan (2014) finds a similar result in the context of other boilerplate consumer contracts.").

[153] Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 1–4 (2009) (describing the FTC consent order against Sears for the tracking of its customers' online behavior even though the customers had checked a box agreeing to Sears' user agreement and privacy policy.).

activities despite those consumers agreeing to a detailed user agreement that explained the tracking procedure.[154]

Another objection to the validity of the contract between consumers and technology companies is the idea of the Privacy Paradox. This "refers to the inconsistencies "between individuals' [asserted] intentions to disclose personal information and [individuals'] actual … disclosure behaviors."[155] The thought is that because consumers say they want privacy, yet behave in contradictory ways, there must be some fundamental defect with these types of contractual transactions.[156]

Much literature has been dedicated to addressing the cause of this paradox.[157] However, the easiest explanation is that there is no paradox; the willingness to surrender privacy is purely indicative of the worth that consumers place on their privacy, which is outweighed by the services they receive.[158] This is known in economics as the revealed preference theory, which posits that the observable behaviors of a consumer are the best indicators of their preference.[159] For example, consider a consumer who purchases a pound of grapes. Revealed preference theory would understand that customer to prefer that pound

---

[154] *Id.*

[155] Holland, *supra* note 147, at 893 (quoting Patricia A. Norberg et al., *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, 41 J. CONSUMER AFF. 100, 100 (2007)).

[156] *See* Kevin E. Davis & Florencia Marotta-Wurgler, *Contracting for Personal Data*, 94 N.Y.U. L. REV. 662, 686–89 (2019) (discussing how the Privacy Paradox could account for an information barrier that leaves consumers unable to make informed decisions to contract); Holland, *supra* note 147, at 902 (discussing how some believe the Privacy Paradox presents market failures in the market for personal information).

[157] Holland, *supra* note 147, at 893 ("The precise contours and causes of the [privacy] paradox are quite controversial.").

[158] Adam Thierer, *Zuckerberg, Facebook & the Privacy Paradox*, THE TECHNOLOGY LIBERATION FRONT (Jan. 15, 2010), https://techliberation.com/2010/01/15/zuckerberg-facebook-the-privacy-paradox/ [https://perma.cc/CFV4-SBV7] (quoting LARRY DOWNES, THE LAWS OF DISRUPTION 80 (2009) ("We do value privacy. It's just that we're willing to trade it for services we value even more.")).

[159] Will Kenton, *Revealed Preference*, INVESTOPEDIA (Aug. 23, 2019), https://www.investopedia.com/terms/r/revealed-preference.asp [https://perma.cc/3XTE-9KVY] ("[C]onsumer behavior, if their income and the item's price are held constant, is the best indicator of their preferences.").

of grapes to all other items that are of the same cost or less.[160] In the context of Behavioral Advertising, consumers who use internet services at the cost of their privacy must prefer those services over their preference for privacy.

Alternatively, another explanation of the privacy paradox is that the paradox is based on the logical fallacy of false equivalence. The Privacy Paradox commits this flaw by comparing consumer attitudes, which focus on general values spanning multiple contextual situations, to behaviors, which focus on specific contextual situations.[161] By comparing peoples' general attitudes to specific behaviors, one can create a paradox through most situations.[162] People say they want to be fit, yet they engage in unfit behaviors.[163] People feel saving money is important, yet many engage in fiscally irresponsible behavior.[164] The fact that general attitudes and behaviors do not line up does not necessarily require reconciliation.

Furthermore, it is possible the difference in consumer behavior and their desire for increased privacy control is not as great as the Privacy Paradox suggests. A recent survey study shows that those who care more about their privacy are more likely to take the time to read the online privacy policies.[165] The study also shows that such privacy

---

[160] *Id.* ("[C]onsider consumer X that purchases a pound of grapes. It is assumed under revealed preference theory that consumer X prefers that pound of grapes above all other items that cost the same, or are cheaper than, that pound of grapes.").

[161] Daniel J. Solove, *The Myth of the Privacy Paradox*, 89 GEO. WASH L. REV. 1, 3 (2021) ("[C]ommentators respond to the privacy paradox by trying to explain away the variance between attitudes and behavior.").

[162] *Id.* ("[C]ommentators argue that the people's behavior is irrational or inconsistent with their actual preferences.").

[163] AMUDHA S. POOBALAN ET AL., BMC PUB. HEALTH, PHYSICAL ACTIVITY ATTITUDES, INTENTIONS AND BEHAVIOUR AMONG 18-25 YEAR OLDS: A MIXED METHOD STUDY, 1, 1 (2012) (finding that "strong intentions to do exercise, was not associated with actual behaviour.").

[164] Melissa M. Cummins et al., *Financial Attitudes and Spending Habits of University Freshmen*, 10 J. ECON. & ECON. EDUC. RES. 3, 17 (finding that 91.5 percent of respondents felt saving money regularly was important, but only 52 percent planned for how to spend their money).

[165] Kesan et al., *supra* note 142, at 296–97 ("Respondents who care more about their personal privacy were more likely to indicate that they read privacy policies ($r = .15$, $p < .01$) and that they have previously refused to use a website because of the website's privacy policy or TOS agreement ($r = .17$, $p < .01$).").

conscious consumers will alter their online behavior as influenced by their privacy and security concerns; some even going so far as to forgo the use of a website altogether.[166] This, coupled with the increasing knowledge of what technology companies do with user data,[167] seems to suggest that informed consumers are well capable of, and do, take privacy into their own hands. If enough informed consumers act, the aggregate results could be economically relevant and would give them the power to drive and change the market.

At the end of the day, paradox or not, data shows that some consumers are largely informed and do take actions to safeguard their privacy.[168] Principles of contract law and autonomy dictate that consumers should have the power to make decisions for themselves and that those decisions should be respected. Perhaps greater access to information and education are needed. However, policy makers should be cautious to push regulations that destabilize the basic tenets of contract law and personal autonomy.

C. Economic Growth, Innovation, and Regulation

Before enacting legislation, it is important to consider the impacts the proposed legislation could have upon economic growth and innovation.[169] After roughly two decades of the FTC's self-regulation approach and guidelines recommending how technology companies can capture and sell user data, a so-called "permissionless" approach to technological innovation has developed.[170] A "permissionless" approach focuses on allowing developers to create and sell new products and services without obtaining permission from the relevant authorities and utilizes an *ex-post* regulation scheme.[171] Contrast this

---

[166] *Id.*

[167] *Id.* at 312 (finding that of all the sections of a data privacy survey, that consumers performed the best in the section testing their knowledge of behavioral advertising practices).

[168] *Id.* at 313 (finding that 66% of survey respondents knew advertisement companies could use their email accounts to personalize advertisements).

[169] Ohlhausen, *supra* note 98, at 3-4 ("Before intervening, regulators must understand how new technologies and business models affect consumers ….").

[170] Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467, 471 (2014) (defining a "permissionless" regulatory approach in contrast with a precautionary one).

[171] Neil Chilson, When Considering Federal Privacy Legislation 9–10 (Dec. 4, 2018) (on file with Regulatory Transparency Project of the Federalist

to a "permissioned" approach where all innovation is closely regulated and must gain regulatory approvals—for example, the pharmaceutical industry.[172] It has been argued that this "permissionless" approach has been one of the largest catalysts for the explosion of technology and internet innovation experienced in the last few decades.[173]

Regulation on the collection and dissemination of user data limits the availability of user data and constrains the methods by which to use that data, bringing the industry into a more permissioned structure.[174] For example, under the CCPA, companies are essentially required to get approval from consumers before using their data in new ways.[175] Proponents of a permissioned approach will point to the safety and comfort of adopting the precautionary principle—exercising caution with new innovations until they can be proven safe.[176] However, the familiar critiques of the precautionary principle: the "threat to technological progress, economic entrepreneurialism, social adaptation, and long-run prosperity" ring especially true in this industry which is so dependent on innovation and speed.[177] Furthermore, application of the precautionary principle can lead to a misallocation of limited resources—diverting resources away from known risks and harms to potential risks and harms, leading to "hazards that

---

Society), https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Privacy-Legislation.pdf (explaining the difference between permissionless and permissioned approaches).

[172] *Id.* ("[A] permissioned approach is one where innovators must seek and receive government approval to pursue an innovation, or where government sets out a specific process that any innovator must follow.").

[173] Thierer, *supra* note 170, at 476 ("This again suggests that [former FTC] Commissioner Ohlhausen's approach to technological innovation is consistent with the permissionless innovation approach that powered the first wave of Internet innovation ….").

[174] Chilson, *supra* note 171 ("[O]verrestricting the use of information about individuals can harm individuals by limiting beneficial information.").

[175] ROPES & GRAY, *supra* note 123 (discussing consumers' right to opt out of data sales immediately upon entering the website).

[176] Thierer, *supra* note 170, at 471 ("[S]ince every technology and technological advance could pose some theoretical danger or risk, public policies should prevent people from using innovations until their developers can prove that they won't cause any harms."); Adam Thierer, *Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle*, 14 MINN. J. L., SCI. & TECH. 311, 353–57 (2013) (highlighting the Congressional concern about the debut of Amazon's Fire tablet and Google's Gmail service).

[177] Thierer, *supra* note 170, at 471.

materialize, or are increased, as a result of regulation."[178] Genuine arguments can be made that these "permissioned" approaches to data privacy generally inhibit technological innovation.[179] Perhaps most persuasive is the specific argument that information-privacy laws impede the flow of information critical to the industry in assessing consumer needs and desires.[180] Thus, keeping this "permissionless" status quo to preserve economic growth and innovation has been one of the main arguments in the literature. But will shifting to a more "permissioned" approach really lead to "fewer services, lower quality goods, higher prices, diminished economic growth, and a decline in the overall standard of living"?[181]

Because much of the proposed data privacy regulation seeks to emulate the EU's robust privacy laws, perhaps the best way to attempt to establish a causal link between such privacy regulation and innovation can be found by comparing the EU and the U.S.[182] Even before the implementation of the GDPR, the EU has had robust privacy protections.[183] In 1995, the EU passed its Directive on the Privacy of Personal Data, which notably: established privacy as a fundamental human right, pushed a consumer notice and choice regime, and favored limitations on the use of consumer data.[184] Contrast this to the U.S., where in 1997 the Clinton Administration stated, "[f]or electronic commerce to flourish, the private sector must lead. Therefore, the Federal Government should encourage industry self-regulation wherever

---

[178] Thierer, *supra* note 176, at 364 (quoting scholar Cass Sunstein, CASS R. SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 102 (2005)).

[179] Tal Z. Zarsky, *The Privacy—Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 139–40 (2015) (discussing the view that regulation can impede both economic innovation and social innovation).

[180] *Id.* at 141–42 ("If information flows are impaired or blocked, innovation will suffer as innovators are unable to use these data flows optimally to produce novel products and services.").

[181] Thierer, *supra* note 170, at 471.

[182] Zarsky, *supra* note 179, at 154 ("In this U.S.-EU comparison, an inescapable linkage between the strength of privacy laws and the level of ICT innovation is evident.").

[183] Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKLEY TECH. L. J. 461, 462 (2000) ("The EU's aggressive regulation of the use of personal data … is embodied in its Directive on the Privacy of Personal Data …, which took effect on October 25, 1998.").

[184] *Id*. at 467–69 (discussing the goals of the Directive and how the Directive seeks to accomplishes these goals).

appropriate ….”[185] Both the U.S. and the EU have mostly kept to these values for the past two decades, and a comparison between the two regimes shows that the U.S. boasts an overwhelming dominance in the information, communications, and technology industries.[186] Furthermore, this disparity exists despite Europe’s high scientific quality, pointing to an inability to apply scientific excellence to business.[187] While opponents of more regulation are quick to point to this as proof of the stifling effects of regulation, it should be noted that a plethora of other differences between the U.S. and EU could have also played some role in the divergent outcomes.[188] These reasons include: lack of a startup culture in the EU, lack of venture capital funding in the EU, the U.S.’s high risk culture, Silicon Valley’s innovation “clusters,” and the U.S.’s “first mover” advantage.[189] While inferring a causative link between innovation and regulation may not currently be possible, the risk to destroying innovation in this industry poses far too great of a danger to the advancement of society, which justifies placing a moratorium on regulation until the innovation-regulation causation can be established with more evidence.[190]

Outside of establishing a causative link between regulation and innovation, what can be conclusively said is that privacy regulation imposes absolute monetary costs.[191] The costs of regulation are quantifiable, direct burdens to industry, and arguably get passed off to

---

[185] Memorandum on Electronic Commerce, 2 PUB. PAPERS 898 (July 1, 1997).
[186] Zarsky, *supra* note 179, at 156 (“[T]he European lag in the ICT realm is a widely discussed phenomenon.”).
[187] *Id*. (“It is part of a broader discussion of the ‘European Paradox’: the vast disparity between Europe’s scientific leadership on the one hand, and its relative innovative failure in the ICT realm on the other.”).
[188] *Id*. at 159–61.
[189] *Id*. (summarizing the main findings of a report written for the EU Joint Research Center).
[190] *See id*. at 166–68 (postulating that the risk to society in social and economic innovations would be too great to justify implementing stringent EU based regulations across the globe).
[191] Alan McQuinn & Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*, INFO. TECH. & INNOVATION FOUND. (Aug. 5, 2019), https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law. [https://perma.cc/H76D-A2CP] (“The Information Technology and Innovation Foundation (ITIF) estimates that if Congress were to pass legislation that mirrors many of the key provisions in the GDPR or the California Consumer Protection Act (CCPA), it could cost the U.S. economy approximately $122 billion.”).

consumers and society at large.[192] For example, in preparing compliance policies for the GDPR, a survey showed that of the companies polled, eighty percent had to spend over $1 million, while forty percent needed to spend over $10 million.[193] The GDPR has also imposed costs to companies through declining revenues, with a new study showing that post-GDPR enactment, websites have had a mean decrease in weekly page views of 11.7% and a decrease in weekly e-commerce recorded revenue of 13.3% for EU users.[194]

Perhaps most importantly, and feeding back into the decline in innovation argument, the GDPR's compliance costs have a disparate impact on smaller firms and discourage startups from entering the market.[195] Compliance costs are usually nonlinear in respect to firm size.[196] Because compliance costs contain fixed costs, larger firms can take advantage of economies of scale regarding these fixed costs, while smaller firms lack this advantage.[197] The GDPR has shown that this lessens competition in the market and has led to a saturation of

---

[192] *Id*. ("[There are] two types of costs associated with a federal data privacy law: compliance costs and market inefficiencies. Compliance costs include personnel companies must hire and capital costs they incur related to new regulations.").

[193] Huddleston, *supra* note 49, at 18 (citing a PricewaterhouseCoopers survey).

[194] Samuel Goldberg et al., Regulating Privacy Online: The Early Impact of the GDPR on European Web Traffic & E-Commerce Outcomes (July 17, 2019) (unpublished manuscript) (available at https://ssrn.com/abstract=3421731) ("Relative to the previous year, we show that recorded pageviews fall by 11.7% and e-commerce recorded revenue falls 13.3% from EU users after the GDPR.").

[195] Eline Chivot & Daniel Castro, *What the Evidence Shows About the Impact of the GDPR After One Year*, CTR. FOR DATA INNOVATION (June 17, 2019), https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/ [https://perma.cc/G95A-KL3W] (showing that between May 2018 and April 2019, monthly EU tech venture deals decreased by 26.1 percent and the average money raised fell 33.8 percent).

[196] C. Steven Bradford, *Does Size Matter? An Economic Analysis of Small Business Exemptions from Regulation*, 8 J. SMALL & EMERGING BUS. L. 1, 18 (2004) ("There is no particular reason to believe the relationships between size and cost or size and benefit are always linear. In fact, there are plausible arguments that those relationships are not linear.").

[197] *Id*. at 14–15 (summarizing that the literature in this field generally shows three findings: 1) that there are economies of scale in regulatory compliance; 2) that the economies of scale deal primarily with fixed costs but also occur with variable costs; 3) that the economies of scale persist over time).

big, well-established technology firms.[198] With Congress's recent antitrust concerns with big technology companies,[199] the potential for these unintended monopolistic effects should be closely analyzed.

Lastly, an estimate of an implementation of the key provisions of the GDPR or the CCPA in the U.S. on a federal level would cost the U.S. economy roughly $122 billion per year or $483 per U.S. adult.[200] In fact, the California Standardized Regulatory Assessment on the CCPA, prepared for the California Attorney General's Office, estimated that the initial compliance costs to California businesses would total approximately $55 billion.[201] At the very least, the prospect of these quantifiable monetary costs should be weighed against the harms and risks associated with keeping or modifying the current regulatory regime.

Further, it is important to note that there are two types of innovations that are considered in this analysis: (1) market innovation, which are the tangible new products that firms are able to offer that directly benefit said firms; and (2) social innovation, which consists of the intangible societal benefits generated from the product and shared through positive externalities or other means.[202] Privacy regulation could stifle both types of innovation; however, social innovation is arguably the more relevant of the two when considering policy.[203] The

---

[198] *See* Huddleston, *supra* note 49, at 24 (identifying the increase in market share for large tech companies after the GDPR's implementation).

[199] Cecilia Kang & David McCabe, *House Lawmakers Condemn Big Tech's 'Monopoly Power' and Urge their Breakups*, NEW YORK TIMES (Oct. 6, 2020), https://www.nytimes.com/2020/10/06/technology/congress-big-tech-monopoly-power.html [https://perma.cc/3M4D-MADZ] (highlighting the House Judiciary Committee's report finding that Amazon, Apple, Facebook, and Google had regularly exercised and abused monopoly power).

[200] McQuinn, *supra* note 191 ("Federal legislation mirroring key provisions of the European Union's General Data Protection Regulation or California's Consumer Protection Act could cost the U.S. economy approximately $122 billion per year, or $483 per U.S. adult.").

[201] DAVID ROLAND-HOLST ET AL., CAL. DEP'T OF JUSTICE, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations* 11 (2019) (observing that the $55 billion is roughly equivalent to 1.8% of California's Gross State Product in 2018).

[202] Zarsky, *supra* note 179, at 126 (distinguishing between market innovations and social innovations).

[203] *Id*. at 142 ("Clearly, establishing whether this dynamic will lead to social innovation, or merely market innovation, is crucial. Just to state the latter is insufficient in the policy realm.").

most important of these social innovations includes free speech, democracy, and the free flow of information.[204]

On a less abstract level, a recent example highlights the benefits of social innovation in the technology sphere: The U.S.' and South Korea's differing responses to the Covid-19 Pandemic. A major part of the successful South Korean response was a heavy emphasis on contact tracing.[205] This involved using cell phone GPS data to track the whereabouts of infected people and then informing those that had been in contact with the infected through text, as well as publishing the relevant GPS location data.[206] The system in South Korea is run by the South Korean government and would likely face constitutional bars if attempted by the federal government. However, private companies would have the ability to implement such policies. In fact, Google and Apple have been constructing such a system, looking to use their technological expertise to provide innovative solutions. However, the system's potential effectiveness and speed of its development have been severely watered down by privacy concerns.[207] The planned systems would rely on Bluetooth due to concerns that GPS tracing would be too invasive, and would require that users explicitly opt-in to

---

[204] *Id*. at 141("[O]ne might argue that ICT-related innovation will lead to 'social innovation' by promoting various social benefits. For instance, the technological infrastructure set in place enables a rich flow of information among citizens and advances free speech and democracy."); Thierer, *supra* note 159, at 352 ("Such information control could stifle free speech, limit the free flow of information, and retard social and economic innovation.").

[205] Max S. Kim, *Seoul's Radical Experiment in Digital Contact Tracing*, NEW YORKER (Apr. 17, 2020), https://www.newyorker.com/news/news-desk/seouls-radical-experiment-in-digital-contact-tracing (describing the extraordinary contact tracing measures taken in South Korea at the onset of the COVID-19 pandemic and how these steps were beneficial in preventing the spread of the virus).

[206] Anthony Kuhn, *South Korea's Tracking of COVID -19 Patients Raises Privacy Concerns*, NPR (May 2, 2020, 8:02 AM), https://www.npr.org/2020/05/02/849535944/south-koreas-tracking-of-covid-19-patients-raises-privacy-concerns [https://perma.cc/KL48-58SX] (discussing the publication of patient-data to prevent the spread of COVID-19).

[207] Russell Brandom & Adi Roertson, *Apple and Google Are Building a Coronavirus Tracking System into iOS and Android*, THE VERGE (Apr. 10, 2020, 12:58 PM), https://www.theverge.com/2020/4/10/21216484/google-apple-coronavirus-contract-tracing-bluetooth-location-tracking-data-app [https://perma.cc/D4ZT-2H7S] (discussing privacy protection measures taken in the development of Apple and Google's system for tracking the spread of the coronavirus).

the program.[208] The reliance on Bluetooth means that both parties—the infected and at risk—would have had to have Bluetooth turned on, and the use of an opt-in over an opt-out system makes it difficult to get the complete and widespread user base that is needed for comprehensive contact tracing.[209] An opt-out, GPS based system would provide a much more comprehensive database and could be an effective method of contact tracing.[210] This is a perfect example of lost social innovation due to excessive precaution over privacy concerns, and illustrates the constraints that a "permissioned" approach could place on innovation.

IV. Recommendations

The previous arguments showcase why additional regulation in this field is unwarranted. However, should more significant threats arise, or public pressure reach a breaking point, regulatory action should focus on enhancing the current framework to address specific needs rather than enacting a comprehensive GDPR or CCPA-based federal approach. Lastly, if states keep passing their own privacy legislation, there may be a need for a federal preemption law to keep the industry from getting bogged down by an unworkable morass of state regulations.

A. Utilizing the Bounds of the Current Framework

In staying within the current regulatory framework, legislators could continue to enhance privacy protections by adding to the piecemeal federal approach. By using a case-by-case *ex post* approach, the priority would be placed on remedying significant harm, allowing the industry to continue to grow and innovate.[211] Adding to this patchwork allows for a balance between commercial and privacy interests across a wide variety of situations and does not try to pigeonhole industry

---

[208] *Id*. (discussing the use of Bluetooth technology and opt-in program to assuage privacy concerns).
[209] *Id*.
[210] *Id*.
[211] Huddleston, *supra* note 49, at 18 ("While this approach is not flawless, the case-by-case ex post approach has allowed a diverse range of data usage and a diverse array of privacy options for consumers while still providing a means of redress when harm does occur.").

under the bounds of an all-encompassing privacy law.[212] This surgical approach allows for privacy laws to remain flexible and adapt with the changes of industry.

Further, the expansion of common law privacy torts is a tool uniquely situated to address the needs of quickly evolving technologies.[213] For example, the tort of private facts could be expanded to protect private or sensitive materials from being disseminated by technology companies.[214] This would be particularly helpful if embarrassing facts about a user did not fall under the protected categories of federal legislation because it would provide redress to those harmed by such disclosures.[215] The tort of intrusion upon seclusion also could be expanded to protect user privacy from unwarranted tracking or spyware. For example, "[i]f data is accessed for an inappropriate purpose, inconsistent with a device manufacturer's privacy policy or consumer expectations, this would lead to consumer harm in the form of potentially intrusive observation."[216] Privacy torts are underutilized and an expansion of their use and acceptance may be warranted. It should be noted that in taking this approach, despite the slow pace of common law development, there is the risk that states adopt differing privacy torts and an unworkable patchwork develops. Even so, a patchwork of state privacy torts would still be preferable to the sweeping and overdemanding state privacy statutes like the CCPA, which would pose the same patchwork problems. Federal preemption of both state common law and legislation, discussed below, would resolve such issues.

---

[212] Ness, *supra* note 47, at 945 ("While this 'patchwork' might be perfectly appropriate for creating a versatile information privacy law that allows for the proper balancing of commercial and privacy interests in different situations ….").

[213] Tran, *supra* note 32, at 295 ("The benefit of common law remedies, however, is that privacy torts can adapt to changing technologies and do not impose the same burdens on regulatory agencies.").

[214] *Id*. at 281 ("This privacy tort is potentially useful because the richness of IoT sensor data may mean this data can be considered 'private facts,' and any publications or disclosures of this data could be considered an invasion of privacy.").

[215] *Id*. at 286–87 (acknowledging that the private facts tort has been successfully applied to "the distribution of intimate sexual information.")

[216] *Id*. at 295 ("If data is accessed for an inappropriate purpose, inconsistent with a device manufacturer's privacy policy or consumer expectations, this would lead to consumer harm in the form of potentially intrusive observation.").

Finally, acting as a catch-all, the FTC, under its Section 5 powers, has addressed a multitude of privacy concerns.[217] The FTC has the ability to enforce data security and ensure that consumers are not being taken advantage of through overinclusive privacy policies. The FTC's Section 5 "unfair and deceptive practices" power is sweeping and broad enough to be adapted to almost any privacy harm that could crop up with new technologies.[218] This is especially important, because the contractual bar to many privacy claims could be overridden, so long as a deceptive or unfair practice could be found.[219] However, the FTC is a large organization with a mandate for consumer protection across all industries, not just tech.[220] A reorganization of the FTC to prioritize consumer protection in the technology industry may be necessary for effective privacy regulation in this area.

B. Federal Preemption

Lastly, an important consideration with legislating technology and internet companies in general is the fact that almost any state has the ability to impose their laws on the rest of the Union.[221] Because the internet functions without borders, companies that comply with one state's privacy policies will have that same set of policies apply across all other states. We already see this taking effect with the passage of the CCPA. If enough states pass their own privacy laws, like have

---

[217] Ohlhausen, *supra* note 98, at 7–8 ("For example, the FTC has brought a broad selection of enforcement cases addressing consumer harms related to the Internet, including more than 100 spam and spyware cases and 50 data security cases.").

[218] Thierer, *supra* note 35, at 449 ("The FTC's authority to police 'unfair and deceptive practices' under Section 5 provides the agency with a remarkably sweeping consumer protection tool to address privacy and data security matters.").

[219] Gindin, *supra* note 153, at 1–3 (explaining that the FTC does not consider the enforceability of contracts but rather whether they are unfair or deceptive such that consumers may be harmed).

[220] Kesan & Bashir, *supra* note 142, at 284 ("[T]he FTC is a very busy agency, and the biggest problem with relying on the FTC to protect consumer privacy is that the FTC often relies on the companies to establish their own standards for how to handle consumer information.").

[221] Huddleston, *supra* note 49, at 19 (explaining that while some "technologies can be retained within borders, this is typically not true when it comes to data driven services.").

been proposed,[222] this could lead to an unworkable patchwork with ballooning compliance costs.[223] Companies that could not afford to comply with all regimes would be forced to choose which states to comply with, probably choosing the most populous states, or just complying with the strictest set of policies.[224] This may lead to states like California dictating what the privacy laws will be for the rest of the country. Further, it seems likely to result in a large decline in competition in the technology industry by pushing out smaller players unable to comply with a multitude of rules.[225] Because of this, some sort of federal preemption should be passed regardless of whether a comprehensive federal privacy law is passed.

V. Conclusion

The outcry for the need to regulate consumer data collection is largely overblown, and lawmakers need to carefully reevaluate the efficacy of the current regulatory scheme before launching into the conclusion that additional restrictive legislation is necessary. Most of the harm arising from within the technology industry can be addressed through existing law, without taking on the impossible task of regulating subjective harms motivated by consumer feelings. Further, evidence seems to suggest that most consumers in this space are aware of the data collection costs for the services they use, and are willing, if not eager, to accept them. Lastly, the loss in economic growth, and more importantly, technological innovation and its positive externalities require serious consideration.

---

[222] Green, *supra* note 22 (listing proposed state privacy laws).
[223] Huddleston, *supra* note 49, at 19 ("New companies might struggle to acquire customers or users if they were unable to offer their product in a widespread manner because of compliance costs while existing large players would more easily be able to absorb such costs.").
[224] *Id*. (acknowledging that upstart companies will struggle with the costs of compliance with a variety of state privacy laws).
[225] *Id*. at 20.