Georgia Law Review

Volume 57 | Number 2 Article 10

3-9-2023

Privacy Is Not Dead: Expressively Using Law to Push Back Against Corporate Deregulators and Meaningfully Protect Data Privacy Rights

Alexander F. Krupp
University of Georgia School of Law, alexander.krupp@uga.edu

Privacy Is Not Dead: Expressively Using Law to Push Back Against Corporate Deregulators and Meaningfully Protect Data Privacy Rights

Cover Page Footnote

* J.D. Candidate, 2023, University of Georgia School of Law; B.A., 2017, University of Kentucky. I would like to thank Professor Thomas E. Kadri for his guidance and insights throughout the process of writing this Note. I would also like to thank the editorial staff at the Georgia Law Review for their efforts. And above all, I thank Penn Hansa for her unwavering support and patience.

PRIVACY IS NOT DEAD: EXPRESSIVELY USING LAW TO PUSH BACK AGAINST CORPORATE DEREGULATORS AND MEANINGFULLY PROTECT DATA PRIVACY RIGHTS

Alexander F. Krupp[*]

When the European Union's (EU) General Data Protection Regulation (GDPR) passed in 2016, it represented the world's first major comprehensive data privacy law and kicked off a conversation about how we think about the right to privacy in the modern age. The law granted a broad range of rights to EU citizens, including a right to have companies delete data they collect about you, a right not to have your personal information sold, and a range of other rights all geared towards individual autonomy over personal data.

All the while, platform companies like Facebook (Meta), Apple, and Amazon have taken advantage of a phenomenon called spontaneous deregulation to outrun legislation designed to regulate data privacy. Spontaneous deregulators take advantage of the inherent gap between the speed at which technology advances and the comparatively languid pace at which legislatures try to keep up. The deregulators do this through co-opting discourses about privacy and pitching a self-regulatory system in which they are entrusted with personal data that they have an inherent profit motive to capitalize on. In today's economy, data is eminently valuable—trusting a system of deregulation creates unacceptable conflicts of interest at best and a predatory system of data mining at worst.

This Note advocates for robust privacy legislation that takes full advantage of the expressive function of the law—the aspect of lawmaking that shapes and protects valuable social norms—to meaningfully protect individual data privacy rights from

[*] J.D. Candidate, 2023, University of Georgia School of Law; B.A., 2017, University of Kentucky. I would like to thank Professor Thomas E. Kadri for his guidance and insights throughout the process of writing this Note. I would also like to thank the editorial staff at the *Georgia Law Review* for their efforts. And above all, I thank Penn Hansa for her unwavering support and patience.

corporate deregulators. By placing social values and human rights at the forefront, expressive law makes it more difficult for deregulators to obfuscate the purposes and messaging of privacy.

TABLE OF CONTENTS

I. INTRODUCTION 878

II. BACKGROUND 885
A. WHAT IS PRIVACY? 885
B. PRIVACY IN THE UNITED STATES 887
C. INTERNATIONAL PRIVACY 890
D. SPONTANEOUS DEREGULATION 892
E. THE EXPRESSIVE FUNCTION OF LAW 895

III. ANALYSIS 896
A. THE PROBLEM TODAY 896
B. WHAT CURRENT LAW GETS RIGHT AND WRONG 901
C. RECOMMENDATIONS 908
1. Data Privacy as a Right in Itself 912
2. Personal Liability 912
3. A Private Right of Action 913
4. Fines 913
5. Opt-In Consent 913
6. Lessons from GDPR 913
7. Progressive Regulation 914
D. ADDRESSING SOME COUNTERARGUMENTS 915

IV. CONCLUSION 917

I. INTRODUCTION

2018 was a big year for data privacy. In March, it came to light that data consulting firm Cambridge Analytica acquired and used the personal information of eighty-seven million Facebook users over the better part of the previous decade to build behavioral profiles on potential voters without their consent.[1] This sparked global outrage and condemnation, forcing Facebook Chief Executive Officer Mark Zuckerberg to apologize and testify before Congress.[2] In May, the European Union's (EU's) widely anticipated General Data Protection Regulation (GDPR) went into effect.[3] This comprehensive data privacy law went further than any law before it, granting sweeping rights to EU citizens regarding their personal information based on the concept that protection of personal information and data "is a fundamental right."[4] In June, California passed the California Consumer Privacy Act (CCPA).[5] Though its focus was narrower than the GDPR's and centered primarily on

---

[1] *See* Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (March 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (reporting on the scandal).

[2] *See Mark Zuckerberg's Wednesday Testimony to Congress on Cambridge Analytica*, POLITICO (Apr. 11, 2018), https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978 (providing a transcript of Zuckerberg's testimony and apology).

[3] *See* Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ (last visited Feb. 24, 2023) (explaining the release and purpose of the GDPR—notably that, through it, "Europe is signaling its firm stance on data privacy and security at a time when more people are entrusting their personal data with cloud services and breaches are a daily occurrence").

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1, 1 [hereinafter GDPR], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[5] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–199.100 (West 2022). The law lays out a set of rights for California consumers, e.g., the right to know what information is being collected, § 1798.100(a)–(b), the right to know if personal data is disclosed to third parties, § 1798.110(a)(4), the right to prevent the sale of personal data to third parties, § 1798.120(b), and a general right of nondiscrimination, § 1798.125(a)(1).

economic concerns, the CCPA represented the first major comprehensive U.S. data privacy law.[6]

These events transformed the international conversation about privacy—today, people care about their online data in ways that were simply not on the public's radar as recently as five years ago.[7] But even so, technology can be difficult to regulate.[8] The field's rapid change makes it easy for lawmakers to fall behind companies like Facebook, Apple, Google, and other "Big Data" purveyors.[9] In sum: technology moves fast and regulations do not.

---

[6] *See* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (Jun. 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html (explaining how, at the time, the CCPA was "one of the most comprehensive [privacy measures] in the United States").

[7] *See* Thomas C. Redman & Robert M. Waltman, *Do You Care About Privacy as Much as Your Customers Do?*, HARV. BUS. REV. (Jan. 28, 2020), https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do (noting that thirty-two percent of survey respondents said that they "care about privacy, are willing to act, *and* have done so by switching companies or providers over data or data-sharing policies"); Venky Anant, Lisa Donchak, James Kaplan & Henning Soller, *The Consumer-Data Opportunity and the Privacy Imperative,* MCKINSEY & CO. (Apr., 2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative (finding that eighty-seven percent of survey respondents "said they would not do business with a company if they had concerns about its security practices" and demonstrating that, largely because of the GDPR, "[a]bout six in ten consumers in Europe now realize that rules regulate the use of their data within their own countries, an increase from only four in ten in 2015"); EY GLOBAL, HAS LOCKDOWN MADE CONSUMERS MORE OPEN TO PRIVACY? 6 (2020), https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/consulting/ey-global-consumer-privacy-survey/ey-data-privacy-report-v2.pdf ("Prior to Covid-19, the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) were already grooming consumers to demand transparency and expect some level of control over their data."); Issie Lapowsky, *How Cambridge Analytica Sparked the Great Privacy Awakening*, WIRED (Mar. 17, 2019, 7:00 AM), https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ ("There has been a growing recognition that companies can no longer be left to regulate themselves, and some states have begun to act on it.").

[8] *See* Daniel Malan, *The Law Can't Keep Up with New Tech. Here's How to Close the Gap*, WORLD ECON. F. (Jun. 21, 2018), https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/ (explaining how technology progresses at a speed that regulation often cannot match and "[b]y the time that a regulation is finally approved, the product or service has changed").

[9] *See* Chanley T. Howell, *Privacy and Big Data*, *in* BIG DATA: A BUSINESS AND LEGAL GUIDE 33 (2015) (explaining that the "primary objective of Big Data is to derive new insights" in ways that are "different from the purpose for which the data was obtained," leading to "issues under the principles of notice and choice, which are fundamental to privacy laws and standards"); Mark Fenwick, Wulf A. Kaal & Erik P.M. Vermeulen, *Regulation Tomorrow:*

The gap between advancing technology and subsequent regulation can be especially damaging because it results in a phenomenon called spontaneous deregulation: when an industry actor takes advantage of a new technology to effectively self-regulate and circumvent existing regulations that are slow to be enacted and slower still to be enforced.[10] Another problem is that these actors can get so far ahead of the regulatory scheme that they begin to influence future regulation, thus shaping it in their own image.[11]

The spontaneous deregulation phenomenon that began at the start of the twentieth century with the proliferation of the automobile and faster lines of communication has exploded in recent years.[12] If left unchecked, spontaneous deregulation creates a "fox in the henhouse" scenario: large industry players who take advantage of existing privacy norms and influence regulation to overlook the loopholes they exploit pose a serious threat to data privacy.[13] Considered in light of the large social and personal harm that breaches of privacy can cause,[14] deregulatory foxes create a serious problem.

What Happens When Technology Is Faster than the Law, 6 AM. U. BUS. L. REV. 561, 567 (2017) (noting that regulators struggle with new technologies "in contemporary settings, where innovation is quicker and the global dissemination of that technology is much faster").

[10] *See* Benjamin Edelman & Damien Geradin, *Spontaneous Deregulation*, HARV. BUS. REV. (Apr. 2016), https://hbr.org/2016/04/spontaneous-deregulation (explaining that spontaneous deregulation tends to render laws and regulations obsolete because industry actors can adapt to "new tech-enabled realities" more quickly and flexibly than legislatures can, therefore allowing them to essentially self-regulate).

[11] *See, e.g.*, Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, PROTOCOL (Feb. 19, 2021), https://www.protocol.com/policy/virginia-maryland-washington-big-tech (explaining how Virginia's data privacy law was originally proposed by an Amazon lobbyist).

[12] *See* Edelman & Geradin, *supra* note 10 ("Benign or otherwise, spontaneous deregulation is happening increasingly rapidly and in ever more industries.").

[13] *See* Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, MARKUP https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time (last updated May 26, 2022, 10:33 PM) (reporting that sophisticated lobbying groups funded by Big Tech have played an active role in influencing state privacy legislation, generally with the aim to weaken consumer protections).

[14] For an interesting take on how to think of direct privacy harms, see M. Ryan Calo, *The Boundaries of Privacy Harm,* 86 IND. L.J. 1131, 1133 (2011) (explaining that privacy harms

So where does that leave us? Today, data privacy is a preeminent issue, sparked by flashpoint events like Cambridge Analytica and crystallized by benchmark-setting laws like GDPR. But to date, there is still no comprehensive federal data privacy law or regulatory scheme to protect peoples' data.[15] The patchwork of federal and state laws that do exist are too narrowed and too focused on certain sectors to be broadly effective.[16] Ultimately, they fail to provide adequate protection to individuals' interests and allow industry actors to circumvent regulations through spontaneous deregulation in ways that would be much harder if data privacy was treated more as a fundamental right.

For example, in 2005, a group of plaintiffs sued JetBlue Airlines for selling their personal information, alleging a violation of the Electronic Communications Privacy Act (ECPA).[17] The court dismissed the case because the ECPA was tailored so narrowly that it did not cover the sort of information contemplated by the complaint.[18] This was even though JetBlue admitted to violating *its own* privacy policy by transferring passenger data to third-party research companies without the passengers' consent.[19] Because the law was never intended to apply to the specific conduct in question in the specific way that it occurred, the plaintiffs were left without

---

can be objective, external harms, but also subjective, internal ones that result in anxiety or embarrassment).

[15] *See* Rita Esposito, *Lack of Federal Data Privacy Legislation Leaves US Agencies to Provide Guidance*, THOMSON REUTERS (Jul. 15, 2022), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/data-privacy-federal-guidance/ (explaining how executive regulation has necessarily stepped into the privacy space due to the lack of legislation).

[16] *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ (explaining the patchwork nature of U.S. state-level data privacy laws and why it causes problems for individual privacy).

[17] *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d. 299, 303 (E.D.N.Y. 2005).

[18] *See id.* at 306–07 (holding in part that the ECPA of 1986 protected only against privacy violations by an "electronic communication service," and JetBlue, an airline, did not qualify as such).

[19] *See id.* at 305 ("JetBlue Chief Executive Officer David Neelman [acknowledged] that the transfer had been a violation of JetBlue's privacy policy.").

a remedy.[20] This demonstrates what can happen when privacy law is not adequately tailored modern harms.

The issue is even more prominent in 2023 as state-level privacy laws begin to adapt.[21] This change is even more pronounced internationally with over eighty countries having passed freestanding data privacy laws.[22] Given that new international, comprehensive data privacy laws are constantly changing the privacy landscape, it is important to understand the real and possible impacts of privacy regulation in a modern online world in which the vast majority of people live on the internet. As such, U.S. privacy regulations must be written and enforced effectively and in a way that sends the right messages. Privacy is too important to leave to a retrospective patchwork approach—it demands and deserves more comprehensive and thoughtful protection.

---

[20] *See id.* at 307 ("Although JetBlue operates a website that receives and transmits data to and from its customers, it is undisputed that it is not the provider of the electronic communication service that allows such data to be transmitted over the Internet.").

[21] *See* Anohky Desai, *US State Privacy Legislation Tracker*, INT'L ASS'N OF PRIV. PROS. (Oct. 7, 2022), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (providing an overview of the status of data privacy legislation in each state). It is worth noting, however, that many of these bills have failed to become law and will likely continue to do so, at least in the short term. *Id.* While bipartisan support for a possible federal law exists, it remains to be seen whether current proposals will be effective or realistic. *See* Hayley Tsukayama, Adam Schwartz, India McKinney & Lee Tien, *Americans Deserve More than the Current American Data Privacy Protection Act*, ELEC. FRONTIER FOUND. (July 24, 2022), https://www.eff.org/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act (noting that the potential law risks preempting more stringent state laws and fails to implement important individual rights).

[22] *See Data Protection Laws of the World*, DLA PIPER, https://www.dlapiperdataprotection.com/ (last visited Jan. 18, 2023) (providing an overview of global data protection laws). Many such laws are shaped in the image of GDPR. Notably, Brazil's General Law for the Protection of Personal Data (LGPD) expressly protects "the essential rights of freedom and privacy and the free development of the personality of the individuals." Lei Geral de Proteçáo de Dados Pessoais, Law No. 13,709/2018. For a summary of Brazil's law, see Sarah Rippy, *An Overview of Brazil's LGPD*, INT'L ASS'N OF PRIV. PROS. (Sept. 18, 2021) https://iapp.org/news/a/an-overview-of-brazils-lgpd/ (noting how the law is "greatly influenced by the EU General Data Protection Regulation"). China's Personal Information Protection Law, enacted on September 1, 2021, is a more significant recent development that "recalls Europe's GDPR in setting a framework to ensure user privacy." Josh Horwitz, *China Passes New Personal Data Privacy Law, To Take Effect Nov. 1*, REUTERS (Aug. 20, 2021, 4:46 AM), https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/.

Here, we have a problem where modern technology reforms the way people and governments ought to think about privacy while simultaneously rendering privacy vulnerable to spontaneous deregulation. What is the law to do? This Note proposes an approach to data privacy legislation that utilizes the expressive function of the law—the way the law sends bigger messages and signals to society beyond just regulating actions[23]—to protect data privacy and curb spontaneous deregulation more effectively. Meaningful change will occur by treating data privacy as a core value and a fundamental right as it has been treated both globally and in certain narrow sectors in the United States.

If you are a U.S. citizen, your credit data is protected by the Fair Credit Reporting Act (FCRA)[24] and your health data is protected by the Health Insurance Portability and Accountability Act (HIPAA) and its Privacy Rule.[25] Those under eighteen have comprehensive privacy protections as well.[26] This patchwork is a hallmark of American data privacy law, the result of a pattern where "legislators are reluctant to impose regulatory requirements on private industry in the absence of market failure."[27] If you happen to live in one of the few states that have passed a comprehensive data privacy law,[28] then your consumer data is somewhat protected. On the whole, however, data privacy in the U.S. is like the Wild West. This is a dangerous mistake.

It is easy to see why sector-specific privacy regulations occur. Few would contend that it is appropriate for your doctor to simply give away your sensitive health information.[29] But a company like

---

[23] For a discussion about the law's expressive function, see Cass R. Sunstein, *On the Expressive Function of Law,* 144 U. PA. L. REV. 2021, 2028 (1996) (noting the importance of law's expression function by pointing out that "[w]hen the [Supreme] Court makes a decision, it is often taken to be speaking on behalf of the nation's basic principles and commitments").

[24] Fair Credit Reporting Act, 15 U.S.C. § 1681–1681(x).

[25] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.); HIPAA Privacy Rule, 45 C.F.R. §§ 160, 164 subpart A, E (2020).

[26] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506.

[27] JAY P. KESAN & CAROL M. HAYES, CYBERSECURITY AND PRIVACY LAW IN A NUTSHELL 228 (2019).

[28] For a list of the privacy laws in each state, see Desai, *supra* note 21.

[29] *See* U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4–9 (2005), https://www.hhs.gov/sites/default/files/privacysummary.pdf (explaining the limited

Google could just as easily use your data without your permission by showing you ads based on your email's contents.[30] Data privacy abuse by deregulators is less obvious than health data intrusions, but such abuse is just as invasive.[31]

Law's expressive function offers better protection. While not a perfect solution, the EU's GDPR enshrines privacy values in a more effective way than have American data privacy laws by using aspects of law's expressive function. By learning from this approach, U.S. regulators should fashion a data privacy approach that is more coherent, more reflective of social norms, and more effective in addressing spontaneous deregulation.

This is not, however, to make any sort of constitutional data privacy right argument. Such a case is valid and relevant but beyond the scope of this Note. Rather, this Note focuses on the unique issue of data privacy, the consequences of doing it wrong, and how to do right. For purposes of this Note, the privacy at issue is more narrowly tailored than what has dominated both American privacy scholarship and jurisprudence. When someone mentions the words "privacy" and "law," seminal cases like *Griswold v. Connecticut*[32] and *Roe v. Wade*[33] may come to mind, and rightly so. But these cases primarily cover government intrusions, whereas this Note is concerned with data privacy violations made by private actors.

Privacy covers many areas, but at its core, data privacy operates as a subset of information privacy.[34] "Privacy has been defined as

---

circumstances in which a covered entity would be allowed to disclose personal health information).

[30] Google previously did this. *See* Selena Larson, *Google Will No Longer Read Your Emails to Tailor Ads*, CNN BUS. (June 23, 2017), https://money.cnn.com/2017/06/23/technology/business/google-ad-scanning-email-stop/index.html (noting the company's decision to cease the practice in response to privacy-related criticism).

[31] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000) (relating informational privacy with "important values concerning the fair and just treatment of individuals within society").

[32] 381 U.S. 479 (1965).

[33] 410 U.S. 113 (1973).

[34] *See* PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY 2 (2020) (identifying information privacy as being "concerned with establishing rules that govern the collection and handling of personal information," as opposed to "bodily privacy" or "territorial

the desire of people to freely choose the circumstances and the degree to which individuals will expose their attitudes and behavior to others" and is "used as a means to protect an individual's independence, dignity and integrity."[35] This is where data privacy in the context of personal data really comes in: when private actors access and misuse personal data, they violate privacy's core.

This Note begins, in Section II.A.1–3, by attempting to define privacy and examining the historical and philosophical bases of data privacy protection in the U.S. and Europe to establish the values that should guide privacy discussions. Section II.A.4 explains the threat spontaneous deregulation poses to modern data privacy, followed by a brief discussion of expressive law in Section II.A.5. Sections III.A–B discusses problems with U.S. privacy law and how personal information is ripe for abuse via spontaneous deregulation. Section III.C then recommends that the U.S. take a comprehensive data privacy approach that takes lessons from the EU and utilizes law's expressive function. It also explains how the approach would more effectively protect personal privacy and prevent the pernicious issue of spontaneous deregulation. Last, Section III.D addresses some of these counterarguments and explain how a comprehensive and expressive approach to data privacy is still the most likely to achieve success and, importantly, to maintain it in a way that protects privacy holistically and sustainably moving forward.

II. BACKGROUND

A. WHAT IS PRIVACY?

The term "privacy" eludes simple classifications—it communicates different things to different people. While it has been often defined as "the right to be let alone,"[36] one study, using a series of interviews with tech company employees, found that common attitudes on privacy differ depending on who is being asked the

privacy," which center on physical invasions, or "communications privacy," which treats as its province the "means of correspondence.").

[35] *Id.* at 1.

[36] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

question.[37] Others define privacy as a question of choice or transparency—of giving the person whose information you are taking the choice of telling you how they do not want that information used.[38] Still others think of privacy in terms of security.[39] But thinking of privacy in these terms risks falling into a dangerous discourse that paints an incomplete picture.[40]

Conceptualizing privacy "in terms of trust" given that "privacy is a facet of social life" provides a richer definition.[41] In this way, privacy defies definition as being any one thing, perhaps to the dismay of judges everywhere. It is best described as a social concept in which an individual entrusts information to another, and that individual's expectations for the extent of that trust form the outer bounds of how the information ought to be used. Privacy as trust incorporates ideas of choice and transparency—few people would argue that transparency is a bad thing. But it grounds privacy as a social norm of a fundamental nature. This is, and must be, an inherently fluid concept, but one that is grounded in ideas not just of consent, but also in terms of trust, basic integrity, and rights. Framing the issue around rights is important, therefore, because it implies that the law is responsible for protecting privacy, not as a checklist item, but as a powerful social norm based on peoples' expectations, not corporations'.

---

[37] ARI EZRA WALDMAN, INDUSTRY UNBOUND: THE INSIDE STORY OF PRIVACY, DATA, AND CORPORATE POWER 12–13 (2021) [hereinafter WALDMAN, INDUSTRY UNBOUND].

[38] *See id.* at 46 ("Others thought privacy was about making choices to disclose information to others.").

[39] Waldman notes that security is about "keeping data secure, preventing leaks and hacks, and . . . other aspects of systems security." *Id. But see* Anant et al., *supra* note 7, at 2 ("Respondents were aware of [data] breaches, which informed their survey answers about trust."). While data privacy and security certainly should not be conflated as one and the same, it would be similarly reductive to look at the two concepts entirely in a vacuum if we are to think about privacy in terms of trust.

[40] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 51 (noting that while much historical scholarship has focused on questions of choice and transparency, privacy is much larger than that).

[41] *Id.*

B. PRIVACY IN THE UNITED STATES

Privacy's importance is certainly not a new concept and it can be seen as a value throughout human history.[42] It was not, however, very widely discussed in the U.S. (at least in academia) until Samuel Warren and future Supreme Court Justice Louis Brandeis wrote *The Right to Privacy* in 1890.[43] There the authors describe a "right to be let alone" that they deem essential "for the protection of the person" in a technologically evolving world.[44] This right, they argued, was not a new one, but simply an extant and "inviolate personality."[45] Warren and Brandeis paved the way for discussion of privacy in the U.S. not as some sort of background concept, but as an individual and fundamental right that ought to be protected.[46] Indeed, Roscoe Pound would go on to note that the article had done "nothing less than add a chapter to our law."[47]

Throughout the twentieth century there remained "considerable confusion concerning the nature of the interest which the right to privacy is designed to protect."[48] As scholars and courts have struggled with this definitional question, comparing it at times to a "haystack in a hurricane,"[49] the advancement of technology has always added urgency to the question.[50] Warren and Brandeis were

---

[42] For a brief note on a few instances of historical examples of the mention of privacy, see SWIRE & KENNEDY-MAYO, *supra* note 34, at 2–3.

[43] Warren & Brandeis, *supra* note 36. The piece was largely written in response to the increased fervor that journalists pursued information about individuals. *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 10 (1979) ("Warren and Brandeis argued that the common law afforded better means to vindicate the right to privacy against newspaperization through legal enforcement . . . .").

[44] *Id.* at 195.

[45] *Id.* at 205.

[46] *See generally* Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990) (discussing the historical impact of Warren and Brandeis's work on the modern right to privacy).

[47] Glancy, *supra* note 43, at 1 (quoting Letter from Roscoe Pound to William Chilton (1916)).

[48] Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 962 (1964).

[49] *Id.* (quoting Ettore v. Philco Television Broad. Co., 229 F.2d 481, 485 (3d Cir. 1956)).

[50] Brooke Auxier, Lee Raine, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-

initially motivated to write about new technology's advent and its use.[51] Writing in the 1960s, Professor Bloustein noted that a study of privacy was "of utmost significance because in our own day scientific and technological advances have raised the spectre of new and frightening invasions of privacy."[52] While this rhetoric gives impressions of demons at the door, it demonstrates that new technologies that change peoples' lives in many positive ways sometimes do so by invading individual privacy expectations.

Presently, the issue seems ever more acute. Brandeis was worried about the invention of instant photography, but one must be curious what he would think about Facebook, Amazon, or Apple. Ever since the advent of mainframe computers in the 1960s, and crescendoing since the internet, more and more information is online.[53] On one hand, easy access to so much information creates "clear and large benefits to individuals and society," but such access simultaneously creates an "unprecedented accumulation of personal data."[54] Companies trading in such data have taken on a preeminent role in modern society, and millions of people use their services every day simply to go about the act of living, whether buying groceries, interacting socially, working, learning, or otherwise.[55] This is particularly true in a post COVID-19 environment, in which existing online is considered more and more *de rigeur*.[56]

---

confused-and-feeling-lack-of-control-over-their-personal-information/ (demonstrating how the modern American data-driven lifestyle has led to increased public concerns over informational privacy).

[51] Warren & Brandeis, *supra* note 36, at 195 ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"). This sounds dramatic today, but the principle stands that new technologies by their nature create privacy concerns.

[52] Bloustein, *supra* note 48, at 963.

[53] *See* Elisa Shearer, *More than Eight-in-Ten Americans Get News from Digital Devices*, PEW RSCH. CTR. (Jan. 12, 2021), https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/ (exemplifying how much modern society depends on the internet for everyday news).

[54] SWIRE & KENNEDY-MAYO, *supra* note 34, at 13.

[55] *See Social Media Factsheet,* PEW RSCH. CTR., (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/social-media/ (noting that over seventy percent of Americans use social media).

[56] *See* John Koetsier, *COVID-19 Accelerated E-Commerce Growth "4 to 6 Years,"* FORBES (June 12, 2020, 10:43 PM), https://www.forbes.com/sites/johnkoetsier/2020/06/12/covid-19-

In today's world, people place their information online to go through the basic motions of life. You can buy groceries on Amazon, pay your bills online with Zelle, or pursue relationships on eHarmony. The question, then, becomes one of autonomy over that information, the dignity that Brandeis's "inviolate personality" represents.[57]

California was the first state to introduce comprehensive data privacy legislation with the CCPA.[58] Virginia and Colorado soon followed.[59] But these laws are limited in their application and scope, focusing primarily on privacy as an economic or consumer protection issue.[60] Moreover, much data privacy enforcement in the U.S. is within the province of the Federal Trade Commission (FTC), an entity openly protecting data privacy as it applies to consumers.[61] The FTC Act itself focuses on "unfair or deceptive acts or practices in or affecting commerce."[62] That idea involves privacy, but the law itself is not *about* privacy—it does not purport to actually protect privacy intrinsically, but instead as a byproduct of general consumer welfare.

---

accelerated-e-commerce-growth-4-to-6-years/?sh=45d7a8ea600f (commenting that e-commerce sales jumped fifty-two billion dollars year-over-year in 2020); Colleen McClain, Emily A. Vogels, Andrew Perrin, Stella Sechopoulos & Lee Rainie, *The Internet and the Pandemic*, PEW RSCH. CTR. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/ (finding that ninety percent of U.S. adults surveyed considered the internet to be "essential or important" to them during the pandemic, with fifty-eight percent considering it to be "essential"); Sarah Perez, *COVID-19 Pandemic Accelerated Shift to E-commerce by 5 Years, New Report Says*, TECHCRUNCH (Aug. 24, 2020, 11:42 AM), https://techcrunch.com/2020/08/24/covid-19-pandemic-accelerated-shift-to-e-commerce-by-5-years-new-report-says/ (finding that the pandemic significantly accelerated the trend of commerce moving online).

[57] *See supra* note 45 and accompanying text.

[58] CAL. CIV. CODE § 1798.100–199 (West 2022).

[59] *See supra* note 21 and accompanying text.

[60] *See, e.g.*, CAL. CIV. CODE § 1798.140(d)(1) (explicitly defining a covered "business" as a for-profit entity that must meet certain revenue traffic thresholds).

[61] *See* THE FEDERAL TRADE COMM'N, https://www.ftc.gov/ (identifying the agency's motto as: "Protecting America's Consumers").

[62] Federal Trade Commission Act, 15 U.S.C. § 57b.

C. INTERNATIONAL PRIVACY

Institutional actors outside of the U.S. have generally taken a more assertive and open approach to data privacy. While much of the U.S. privacy legal infrastructure is based on common law[63] or sectoral statutory law,[64] international sources have been much more explicit and direct. For example, the immensely influential Universal Declaration of Human Rights explicitly asserts that "no one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence."[65] And the UN has not exactly been shy about data privacy since. A further feature of European privacy law that predates the GDPR is that it "broadly protects against infringements by private parties,"[66] as opposed to American privacy law that often targets specific areas like healthcare or education.[67]

In 2021, the UN High Commissioner for Human Rights urged for stringent measures treating privacy as a well-established international human right.[68] In Europe specifically, personal data has been protected in some form since 1981 with the passage of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[69] That treaty "protects the individual against abuses which may accompany the collection and processing of personal data."[70] Then, in 1995, the EU passed the

---

[63] Indeed, Brandeis's germinal piece advocating for a right to privacy explicitly contemplated its enforcement entirely through existing common law. *See* Warren & Brandeis, *supra* note 36, at 198. It is worth noting, however, that certain states do have a right to privacy enshrined in their constitutions. *See, e.g.*, CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . pursuing and obtaining safety, happiness, and privacy.").

[64] *See supra* notes 24–28 and accompanying text.

[65] G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at 25 (Dec. 10, 1948).

[66] KESAN & HAYES, *supra* note 27, at 227.

[67] *See supra* notes 24–28 and accompanying text.

[68] *See* U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age,* U.N. Doc. A/HRC/48/31, at 15 (Sept. 15, 2021) (recommending states impose moratoriums on the sale and use of artificial intelligence systems that carry a high risk for the enjoyment of human rights).

[69] Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108, 1496 U.N.T.S. 65.

[70] *Id.* at 66–67.

Data Protection Directive.[71] This document expressly states that data processing is "designed to serve man" and, in doing so, must "respect their fundamental rights and freedoms, notably the right to privacy."[72]

Vice President of the European Commission Viviane Reding first proposed the GDPR in a speech to the European Commission, framing the issue as "a question of individuals' rights being overridden by technological change" and vowing that the law would move forward because "people should see that their rights are enforced in a meaningful way."[73] The GDPR was passed into EU law in 2016[74] and became effective in 2018.[75] The law lists a series of data rights, such as the right to have personal data deleted[76] and the right to be informed (with information provided in a "concise, transparent, intelligible, and easily accessible form"),[77] as well as a series of "key principles" like data minimization.[78] While the GDPR has some similarities to CCPA, it is stricter and more comprehensive, exhibiting a more aggressively expressive European data privacy regime compared to American law.[79] This does not, however, mean that it is infallible. While its tone treats data privacy like a human right, much of the underlying text is similarly commercial to CCPA, and many of the loopholes present in CCPA are also present in GDPR.[80]

---

[71] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, art. 25, 1995 O.J. (L 281) 31, 31.

[72] *Id.*

[73] Viviane Reding, Vice-President, Eur. Comm'n, Speech: A Data Protection Compact for Europe (Jan. 28, 2014), https://ec.europa.eu/commission/presscorner/detail/de/SPEECH_14_62.

[74] GDPR, *supra* note 4, at 87–88.

[75] Wolford, *supra* note 3.

[76] GDPR, *supra* note 4, at 43.

[77] *Id.* at 39.

[78] *Id.* at 35.

[79] *See* 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, 111–15 (2019) ("The GDPR's requirements have been interpreted as being more stringent than the CCPA's.").

[80] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 106–07 (comparing the CCPA with the GDPR and noting deficiencies in each). In a twist of spontaneous deregulation-flavored irony, in the early drafting of GDPR, American corporate actors influenced the more business-friendly aspects of the law and toned it down from what it potentially could have been. *See*

D. SPONTANEOUS DEREGULATION

Data privacy is generally broken down into two different arenas: (1) government surveillance of citizens and (2) collection and use by private commercial actors.[81] This Note concerns the latter—that is where spontaneous deregulation comes in. Spontaneous deregulation has existed as a concept ever since technology and regulation first began to butt heads but was only named for the first time in 2016.[82] The phenomenon occurs when "successful platform businesses" engage in "rule flouting" to take advantage of the gap between regulation and the new realities their technologies enable. While certain business strategies can cope with spontaneous deregulation in competitive markets, the concept illuminates how privacy is vulnerable to exploitation by business.[83]

Technology moves faster than law does.[84] This is not surprising. On one hand, technology is synonymous with innovation: it was designed to move fast and solve problems aggressively.[85] On the other hand, the founders designed Congress to do just the opposite: it moves slowly and deliberately with an intentional process designed to prevent rash laws with dire consequences.[86] This can

---

Francesco Guarascio, *US Lobbying Waters Down EU Data Protection Reform*, EURACTIV (Feb. 21, 2012), https://www.euractiv.com/section/digital/news/us-lobbying-waters-down-eu-data-protection-reform/ ("The lobbying was successful since eventually the final text issued by the Commission takes on board many of the concerns raised by Washington.").

[81] *See* KESAN & HAYES, *supra* note 27, at 227 ("[T]he first major category of privacy law concerns protection of citizens from the government. The second concerns protecting citizens from having their privacy violated by other citizens.").

[82] *See* Edelman & Geradin, *supra* note 10 ("This rule flouting is a phenomenon we call 'spontaneous private deregulation,' and it is not new.").

[83] *See id.* (discussing how spontaneous deregulation causes harms in various business contexts).

[84] *See id.* ("Innovation has often rendered laws and regulations obsolete.").

[85] *See* Greg Satell, *Why "Move Fast and Break Things" Doesn't Work Anymore*, HARV. BUS. REV. (Dec. 10, 2019), https://hbr.org/2019/12/why-move-fast-and-break-things-doesnt-work-anymore ("For the past few decades, agility in the technology sector has largely meant moving faster and faster a predetermined path; innovation has largely been driven by our ability to cram more transistors onto a silicon wafer.").

[86] *See, e.g.*, Michael J. Gerhardt, *Why Gridlock Matters*, 88 NOTRE DAME L. REV. 2107, 2107 (2013) ("Antonin Scalia, the longest serving justice on the current Supreme Court, told the Senate Judiciary Committee that, 'Americans should learn to love gridlock. . . . The framers (of the Constitution) would say, yes, "That's exactly the way we set it up. We wanted power contradicting power (to prevent) an excess of legislation."'").

create an issue when legislators decide to regulate technology.[87] They cannot keep pace, and even if they sometimes can, the regulations are ineffective or haphazard.[88] This contrast creates an environment in which corporate actors "see [regulations] as unwanted holdovers from a bygone era not yet ready for their innovations."[89] Early examples include the invention of the automobile and the airplane.[90] In modern society, businesses understand the opportunity presented by spontaneous deregulation and can exploit it by simply innovating around regulations.[91]

Uber, for example, noticed taxi services' disadvantages: they can be inefficient, slow, and costly, partially due to how they are regulated, and they simply do not go everywhere, particularly for people in cities without a heavily developed transportation infrastructure.[92] The idea that normal people could use a service and be ferried around by other people in the community has created advantages for everyday people just trying to get from point A to point B.[93] But sometimes regulation exists for a reason.[94]

And in an entirely unregulated space, corporations can stand to make a massive profit from their innovations while leaving ordinary people vulnerable to gaps left unfilled.[95] Uber itself has dealt with several highly publicized incidents related to its "move-fast-and-

---

[87] *See* Marci Harris, *Here's What Happens When Tech Outpaces Government*, APOLITICAL (Sept. 12, 2019), https://apolitical.co/solution-articles/en/heres-what-happens-when-tech-outpaces-government (describing the range of "pacing problems" Congress must cope with to "keep up with the scope and speed of technological change in industry and society").

[88] *See, e.g.*, *id.* ("And we all remember the infamous Facebook hearings, revealing 'how little Congress seems to know about Facebook, much less what to do about it.'").

[89] Edelman & Geradin, *supra* note 10.

[90] *See id.* ("[T]he budding automobile and aviation industries faced similar challenges.").

[91] *See id.* (illustrating examples like Napster, YouTube, Uber, Airbnb, and food delivery).

[92] *See* John Greil, *The Unfranchised Competitor Doctrine*, 66 VILL. L. REV. 357, 366–69 (2021) (examining taxi markets and their traditional regulations and Uber's emergence).

[93] *See id.* at 369–75 (noting Uber's transition from a "high-end black car service" to providing more basic offerings).

[94] *See* Edelman & Geradin, *supra* note 10 ("Many people with disabilities can't use Uber or Lyft because those services do not have to guarantee wheelchair accessibility, unlike taxi fleet firms in most U.S. jurisdictions.").

[95] *See generally* William Lazonick, *Profits Without Prosperity,* HARV. BUS. REV. (Sept. 2014), https://hbr.org/2014/09/profits-without-prosperity (tracking the trend of high corporate profits in recent years).

break things approach."[96] A particularly relevant example was the company's experiment with "God View," which let Uber employees track customers in real-time without "basic security practices."[97]

Privacy is particularly vulnerable to the threat of spontaneous deregulation that arises where innovators "find ways to leverage the underused capabilities or assets of private individuals, realizing both lower costs and greater flexibility."[98] In our case, those "assets" are people and their personal data. While spontaneous deregulation is not always harmful,[99] spontaneous deregulation by Big Tech companies in the privacy arena actively threatens individual autonomy and integrity.

While legislators have long been aware of these privacy issues,[100] Congress has consistently struggled to attack the issue coherently and effectively.[101] Congress's hesitancy and languid approach to

---

[96] Madison Malone Kirchner, *How Uber Got Here,* N.Y. MAG. (Mar. 8, 2017), https://nymag.com/intelligencer/article/dramatic-history-ride-hailing-app-uber-and-ceo-kalanick.html ("[T]he company has faced allegations of sexual harassment, a lawsuit over stolen technology, and a secret dashboard video of CEO Travis Kalanick losing his temper at a driver."). Additionally, the company has been criticized for not adequately protecting customer location data. *See id.* ("At the launch of Uber Chicago, guests are treated to a screen showing—without their permission—the location of 'known people' using Uber in New York. Investor Peter Sims . . . would go on to write a Medium post about the experience in 2014.").

[97] Brian Fung, *Uber Settles with FTC Over Allegations it Failed to Protect Customer Data*, WASH. POST (Aug. 15, 2017, 11:24 AM), https://www.washingtonpost.com/news/the-switch/wp/2017/08/15/uber-is-settling-with-the-ftc-in-a-major-case-over-privacy-and-security/.

[98] Edelman & Geradin, *supra* note 10.

[99] Deregulation helped to liberalize ideas around automobile driving in the 19th Century, for example. *See id* (describing the phenomenon).

[100] *See, e.g.,* Press Release, Richard Blumenthal, "MY DATA" Bill to Defend Online Privacy (Apr. 27, 2017), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-udall-introduce-my-data-bill-to-defend-online-privacy (exemplifying one of many efforts made by congresspeople in the past to pass data privacy legislation).

[101] *See* Jessica Rich, *After 20 Years of Debate, It's Time for Congress to Finally Pass a Baseline Privacy Law*, BROOKINGS (Jan. 14, 2021), https://www.brookings.edu/blog/techtank/2021/01/14/after-20-years-of-debate-its-time-for-congress-to-finally-pass-a-baseline-privacy-law/ (noting that the federal government has dealt with start-and-stop initiatives to regulate information privacy for decades); Chris Kirkham & Jeffrey Dastin, *U.S. Lawmakers Call For Privacy Legislation After Reuters Report on Amazon Lobbying*, REUTERS (Nov. 22, 2021, 10:44 PM), https://www.reuters.com/world/us/us-lawmakers-call-privacy-legislation-after-reuters-report-amazon-lobbying-2021-11-22/ (detailing bipartisan initiatives to introduce privacy

data privacy has left the space wide open for the companies that engage in spontaneous deregulation to take advantage of the vacuum. The best way to address that problem is by utilizing the expressive function of law purposefully and proactively.

E. THE EXPRESSIVE FUNCTION OF LAW

Laws serve many different functions in society. It is a basic premise that the law exists in part to protect people against capricious and malicious actors,[102] but it achieves this in several ways. There is corrective justice, which aims to address and correct past wrongs.[103] This is law acting retroactively. But laws can also work proactively as a deterrent.[104] Finally, law plays a crucial role in both shaping social norms and crystallizing emerging or extant ones via the expressive function of law.[105]

By analyzing legal situations through the lens of its expressive power, we can better acknowledge that law and people do not interact in a rigid binary. Laws can be more than just coercive—they can also be expressions of social discourse (for good or ill), and

---

legislation in response to Amazon efforts to undermine privacy protections, including from lawmakers in states where Amazon has a significant presence).

[102] *See, e.g.,* Arthur Ripstein, *Theories of the Common Law of Torts*, STAN. ENCYC. PHIL. (Jun. 2, 2022), https://plato.stanford.edu/entries/tort-theories/#TortLawHistPhil ("Tort law lays out the minimal forms of conduct that people are legally entitled to demand of each other . . . .").

[103] For more information on the origins of this facet of law, see ARISTOTLE, NICOMACHEAN ETHICS 86–86 (Terence Irwin trans., 3d ed. 2019), in which Aristotle explains human experience as a series of interactions. When interactions create injustice, they create an unfair gain for the guilty party and a loss for the innocent one, and it is for the law to step in and correct this imbalance. *See also* Jules Coleman, *The Practice of Corrective Justice, in* PHIL. FOUNDS. OF TORT L. 53 (David G. Owen, ed., 1995) (arguing that corrective justice is a primary driver of tort law).

[104] *See* Thomas C. Galligan, Jr., *Deterrence: The Legitimate Function of the Public Tort*, 58 WASH. & LEE L. REV. 1019, 1020 (2001) (discussing the deterrent function of tort law as a principal goal of the concept).

[105] *See* Sunstein, *supra* note 23, at 2025–27 (noting both that law can function as a "statement" to affect social norms and "push them in the right direction" and that "society might identify the norms to which it is committed and insist on those norms via law"); Thomas A. J. McGinn, *The Expressive Function of Law and the* Lex Imperfecta, 11 ROMAN LEGAL TRADITION 1, 7 (2015) (finding that the law has a role in "internalization," which concerns "both reinforcing and altering social norms").

that can be powerful.[106] While law's expressiveness can be difficult to measure,[107] data privacy regulation can be used expressively to crystallize social norms to protect privacy and push back against zealous advocates of deregulation like Big Tech. The expressive function of law can deter corporate interest-friendly regulation and guarantee that the law protects data privacy as a legitimate right. Expressive regulation, therefore, creates a system where the actor whose behavior is confirmed as a social value is the citizen and the actor whose behavior is constrained through legal expression is the deregulator.

III. ANALYSIS

A. THE PROBLEM TODAY

Privacy as an issue will not sort itself out; some white knight will not come in and "fix" privacy just because it is an important issue. Spontaneous deregulation is pernicious, subtle, and inherently complicated in its messaging.[108] This is because many of the concerns that deregulators push sound very compelling in a vacuum.[109] For example, it is argued that laws like GDPR stifle innovation and ambition by creating cumbersome compliance requirements.[110]

---

[106] *See* Janice Nadler, *Expressive Law, Social Norms, and Social Groups,* 42 L. & SOC. INQUIRY 60, 60 (2017), (explaining that "group identity interacts with law to provide motivations to comply" and rejecting the idea that law serves only a coercive function).

[107] *See* Patricia Funk, *Is There an Expressive Function of Law? An Empirical Analysis of Voting Laws with Symbolic Fines,* 9 AM. L. & ECON. REV. 135, 137 (2007) ("Although there is scant empirical research on expressive effects of law, legal scholars start taking them for granted."). *But see* Maggie Wittlin, Note, *Buckling Under Pressure: An Empirical Test of the Expressive Effects of Law*, 28 YALE J. REG. 419, 421–22 (2011) (finding that seat belt laws have an expressive effect and that seatbelt laws with expressive elements generally lead to higher rates of seatbelt adoption).

[108] *See infra* note 228 and accompanying text.

[109] *See* Patrick A. McLaughlin, *A Disruptive Innovation Like Uber is not "Spontaneous Deregulation,"* THE HILL (Jul. 1, 2016, 10:32 AM), https://thehill.com/homenews/286248-a-disruptive-innovation-like-uber-is-not-spontaneous-deregulation/ (championing the innovative qualities of deregulators like Uber).

[110] *See, e.g.*, *The 10 Problems of the GDPR: Hearing on the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Judiciary Comm.*, 116th Cong. 3 (2019) (statement of Roslyn Layton, Visiting Scholar, American Enterprise Institute) ("The data

And the obfuscation of privacy as the main issue persists in a more general sense. Privacy professionals would consistently tout things like anonymization, data breach prevention, and other concepts relating to cybersecurity,[111] and these are good things—nobody wants a data breach. When asked why websites set their privacy settings to the most permissive standard by default, the same professionals touted concepts like efficiency, consumer choice, and so on.[112] And these concepts can create some benefits.[113] Few users want a disjointed experience that requires affirmative action to use a website as efficiently as possible.[114] Spontaneous deregulators focus on the same concepts. Companies like VRBO, the popular vacation rental site, are popular because they are easy and intuitive and free the user from the cumbersome experience and expense of booking a hotel room.[115]

The very nature of the issue's complexity opens it up to expressive messaging on all sides, allowing deregulators to instill a sense of complacency with the status quo. The risk is particularly important with privacy because "privacy" as a concept is not a product in the same way that a car is. This makes it difficult to pin down. When studying privacy, we have to ask ourselves first what it is, and there is no real right answer.[116] But you will be hard-pressed to find many people who need to ask, "what is a car?" This conceptual difficulty, when paired with messaging from deregulators that everything is fine, creates an expressive tapestry

---

show that the EU has not fostered an environment in which small- and medium-sized companies grow.").

[111] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 16–27 (describing various cybersecurity-related approaches that industry professionals take).

[112] *See id.* at 21 (noting in an interview that an employee responded with mostly cybersecurity-related measures when asked what privacy work their tech company did).

[113] *See id.* at 22 (discussing the perceived benefits of a streamlined, efficient user experience when it comes to technology).

[114] *See id. (*highlighting the belief that "you should be able to do everything you possibly want in one app").

[115] *See* Richard W.F. Swor, Note, *Long Term Solutions to the Short-Term Problem: An Analysis of the Current Legal Issues Related to Airbnb and Similar Short-Term Rental Companies with a Proposed Model Ordinance*, 6 BELMONT L. REV. 278, 278 (2019) (explaining how vacation rental sites like Airbnb have revolutionized the industry and have required "cities to revolutionize their laws").

[116] *See supra* section II.A.

leading to complacency as the individual has no reason to believe that the deregulator may be acting with adverse interests.

In the face of tech-focused justifications, privacy is easy to "cast as old-fashioned at best and downright harmful at worst—antiprogressive, overly costly, and inimical to the welfare of the body politic."[117] Often, "when privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser."[118] Thus, deregulators' justifications for dismissing or reducing privacy render it vulnerable to being boxed out as a valuable social norm. This is unfortunate because, just like industry, "privacy also shelters the processes of play and experimentation from which innovation emerges."[119] In other words, privacy is not the inverse of progress—it complements progress.

When asked how they feel about the privacy implications of a product like Amazon's Alexa smart home system, many people will say it bothers them and that they find it invasive.[120] But they are also likely to chalk it up to the price you pay for convenience.[121] Disregarding privacy leads to a new, higher baseline about what is acceptable and about how far into your privacy the deregulator can reach. And the deregulators are actively involved in creating this new baseline. For example, in October 2021, Delta Air Lines announced new facial recognition technology to check airline passengers in their Atlanta hub.[122] Unsurprisingly, some found this

---

[117] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1904 (2013) [hereinafter Cohen, *What Privacy Is For*].

[118] *Id.*

[119] *Id.* at 1906.

[120] Sarah Perez, *41% of Voice Assistant Users Have Concerns About Trust and Privacy, Report Finds*, TECHCRUNCH (Apr. 24, 2019, 3:32 PM), https://techcrunch.com/2019/04/24/41-of-voice-assistant-users-have-concerns-about-trust-and-privacy-report-finds/ (finding that more than half of survey respondents did not trust that their data was secure with digital assistants); DELOITTE INSIGHTS, 2022 GLOBAL MARKETING TRENDS 12, https://www2.deloitte.com/content/dam/insights/articles/us164911_gmt_2022_master/DI_2022-Global-Marketing-Trends.pdf (finding that survey respondents generally react negatively if they feel their device is "listening to them" in order to tailor ads).

[121] In *Industry Unbound*, Waldman quotes Mastercard CEO Ajay Banga who claimed that consumers prefer "convenience over security" because it is simply easier. WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 63.

[122] Kelly Yamanouchi, *Delta to Roll out Facial Recognition in Atlanta Domestic Terminal,* ATLANTA J. CONST. (Oct. 26, 2021), https://www.ajc.com/news/atlanta-airport-blog/delta-to-

unnerving.[123] For its part, the airline claimed efficiency and public health justifications, arguing the technology would make the check-in process easier and contactless.[124] In England, biometric technology is used to reduce cafeteria lines in primary schools, and in China it has even been used to apprehend toilet paper burglars.[125] There is nothing at all wrong about the efficiencies created. But such efficiencies threaten to normalize people "understanding their bodies as something they use to transact," which, in turn, "condition[s] an entire society to use facial recognition."[126]

The same holds true for data online. Facebook founder and Chief Executive Officer Mark Zuckerberg publicly stated he did not consider privacy to be something people expect anymore.[127] And in a California courtroom in 2019, Facebook lawyers attempted to explain to a judge that "[t]here is no privacy interest, because by sharing with a hundred friends on a social media platform, which is an affirmative social act . . . you have just . . . negated any reasonable expectation of privacy."[128] This demonstrates that Facebook's leaders believe, at least in court, that not only is privacy *not* a social norm, but that it is also the consumer's fault that it is

---

roll-out-facial-recognition-in-atlanta-domestic-terminal/ZNLXOB2BSBFDPNJXSWBOJ5S6FU/.

[123] *See* Kelly Yamanouchi, *As Delta Expands Facial Scanning, Opposition to Technology Grows*, ATLANTA J. CONST. (Sept. 17, 2019), https://www.ajc.com/news/delta-expands-facial-scanning-opposition-grows/wI68thmbgXnNUJu4Khwe9J/ (detailing public backlash against facial recognition at airports).

[124] *See id.* ("The goal is to make the travel experience more convenient and 'hands-free and touch-free,' said Greg Forbes, Delta's managing director of airport experience.").

[125] *See* Rob Davies, *"Conditioning an Entire Society": The Rise of Biometric Data Technology*, GUARDIAN (Oct. 26, 2021, 3:00 PM), https://www.theguardian.com/technology/2021/oct/26/conditioning-an-entire-society-the-rise-of-biometric-data-technology (observing incidents in which facial recognition technology has been used in various public settings).

[126] *Id.* (quoting Stephanie Hare, author of Technology Ethics).

[127] *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder,* GUARDIAN (Jan. 10, 2010, 8:58 PM), https://www.theguardian.com/technology/2010/jan/11/facebook-privacy ("People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people . . . . That social norm is just something that has evolved over time." (quoting Mark Zuckerberg)).

[128] Sam Biddle, *In Court, Facebook Blames Users for Destroying Their Own Right to Privacy,* INTERCEPT (June 18, 2019, 11:50 AM), https://theintercept.com/2019/06/14/facebook-privacy-policy-court/.

this way. This is so even in the face of public messaging in which companies tell users that they care deeply about their privacy policy.[129]

Stronger legislation protecting privacy unashamedly and expressively is necessary because privacy is already inherently susceptible to having its messaging co-opted. As data has become more accessible, it has also become more useful, and companies can analyze it to uncover valuable market research more efficiently.[130] For example, Target tracked customer data to determine if a person's prior purchases could predict if they were pregnant, allowing for directed advertising at pregnant women.[131] Target took advantage of the data it could gain from users to build its business.[132] And therein lies the principal issue with deregulating corporations in the privacy space—true privacy is diametrically opposed to their profit incentives.

This is why Facebook makes sure to tell users it cares about their privacy, all the while collecting information and disclosing it to third parties without telling users.[133] It is why companies, both internally and publicly, tout cybersecurity as privacy.[134] But cybersecurity

---

[129] *See* Johana Bhuiyan, *Apple Says It Prioritizes Privacy. Experts Say Gaps Remain,* GUARDIAN (Sep. 23, 2022, 6:00 AM), https://www.theguardian.com/technology/2022/sep/23/apple-user-data-law-enforcement-falling-short (mentioning Apple as an example of a company with active privacy messaging but faulty privacy processes).

[130] *See* James R. Kalyvas & David R. Albertson, *A Big Data Primer for Executives*, *in* BIG DATA: A BUSINESS AND LEGAL GUIDE, *supra* note 9, at 5 ("Today, more than 95% of all data that exists globally is estimated to be unstructured data. . . . [O]rganizations can now make correlations and uncover patterns . . . [that] can provide a company with insight on external conditions that have a direct impact on an enterprise, such as market trends, consumer behaviors, and operational efficiencies, as well as identify interdependencies between the conditions.").

[131] *See* Charles Duhigg, *How Companies Learn Your Secrets,* N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (reporting on Target's tactic for marketing to pregnant women).

[132] *See id.* ("Andrew Pole was hired by Target to use . . . insights into consumers' habits to expand Target's sales.").

[133] *See Facebook's Data-Sharing Deals Exposed*, BBC (Dec. 19, 2018), https://www.bbc.co.uk/news/technology-46618582 ("[Facebook] shared access to users' data with other tech firms, including Amazon, Apple, Microsoft, Netflix, Spotify and Yandex.").

[134] *See, e.g.*, Eileen Guo, *A Roomba Recorded a Woman on the Toilet. How Did Screenshots End Up on Facebook?*, MIT TECH. REV. (Dec. 19, 2022),

protects the user against malicious hackers, not against the company collecting your data.[135]

This phenomenon has been dubbed "informational capitalism," alluding to the use of information as a commodity by companies such as Facebook, Amazon, or Target to make money via "targeted advertisements, search results, and other content."[136] Companies do so subtly, creating new norms and expectations in the consumer,[137] making the phenomenon even more pernicious and important to address.

B. WHAT CURRENT LAW GETS RIGHT AND WRONG

Data privacy law has come a long way in a short time. The CCPA and the GDPR were significant achievements that changed the conversation about data privacy.[138] But the existence of a regulation does not guarantee effective regulation. The CCPA, generally viewed as America's flagship data privacy regulation,[139] risks being "merely performative" and devoid of workable substance that protects peoples' privacy interests.[140]

First, American privacy laws are fragmented, sectoral, and have a neutered expressive impact.[141] It is easy in such an environment

---

https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/ (noting that companies sometimes exploit subtle differences between privacy and security).

[135] *See id.* ("When a company says it will never sell your data, that doesn't mean it won't use it or share it with others for analysis.").

[136] Cohen, *What Privacy Is For*, *supra* note 117, at 1915–16.

[137] *See id.* at 1916 ("The surveillant assemblages of informational capitalism . . . beckon with seductive appeal. Individual citizen-consumers willingly and actively participate in processes of modulation, seeking the benefits that increased personalization can bring.").

[138] *See* Anant et al., *supra* note 7 (noting how European awareness of data privacy rights has gone up significantly since the passage of GDPR).

[139] *See* Kari Paul, *California's Groundbreaking Privacy Law Takes Effect in January. What Does It Do?*, GUARDIAN (Dec. 30, 2019, 3:00 AM), https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do (describing the CCPA as a "landmark privacy law" giving residents "unprecedented" rights).

[140] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 84 ("Better security may calm fears of harm from future data breaches, but it seems orthogonal to a data misuse problem. It's performance: it doesn't hurt, but while it's not actually solving the problem, it is socially constructing *privacy* work as *security* work.").

[141] *See* Klosowski, *supra* note 16 (noting that "[c]urrently, privacy laws are a cluttered mess of different sectoral rules").

for deregulators to occupy unregulated spaces because the very nature of the law creates those spaces like a block of Swiss cheese. This was evident in the *JetBlue* case in which the airline was able to share customer information with third parties due to an overly narrow law.[142]

A patchwork system leaves open possibilities for companies incentivized to use personal data to profit-maximizing ends to do so without flouting any laws because those laws are not expressively designed to combat wider issues. This is true in a purely geographic sense. If a company wishes to avoid being beholden to CCPA, that company simply operates in such a way to not trigger that law's thresholds for enforcement.[143] The lack of statutory expression also communicates that a person who lives outside California, Colorado, or Virginia has no real recourse to general protections of their privacy in a statutory sense.

Technology in the twenty-first century is essentially borderless; it makes little sense to take a state-by-state approach to something that does not check itself at the state border. In addition, by focusing on the "consumer" as essentially all-American data privacy laws do,[144] statutes minimize the role of data privacy in a social sense and do a poor job of reflecting privacy comprehensively and broadly. Instead, due to this singular focus on consumers, statutes are limited narrowly around economic interests. The overly narrow focus of American consumer laws creates gaps for deregulators to

---

[142] *See supra* notes 17–20 and accompanying text.

[143] *See* CAL. CIV. CODE § 1798.140 (West 2022) (providing several qualifying instances where companies could operate outside the CCPA regarding purpose or statutory thresholds). It is also notable that the CCPA consciously leaves out any application to nonprofit entities, and it also does not apply to data given to for-profit entities that are related to non-commercial activities, reinforcing the idea that the law is not focused on people as humans, but rather people as consumers of the services created by for-profit companies. *See, e.g.*, *id.* § 1798.140(c) (defining "business" as an entity "organized or operated for the profit . . . of its shareholders"); *id.* § 1798.100 (detailing the general duties of "businesses" under the CCPA). However, a ballot initiative passed in 2020 called the California Privacy Rights Act (CPRA) took effect January 1, 2023, expanding several data privacy protections and thereby broadening the scope and application of the CCPA. California Privacy Rights Act of 2020 (codified as amended at CAL. CIV. CODE §§ 1798.100–1798.199.100).

[144] *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 115 (2017) (contrasting European privacy culture's focus on rights with American privacy culture's focus on consumers).

operate, and expressive law, with its social focus, can close those gaps.

More specifically, the CCPA and its other state law counterparts have severe deficiencies. In addition to its narrow consumerist scope, the CCPA focuses too intently on transparency and does not differentiate between the types of data it claims to protect.[145] To its credit, the law does have requirements of disclosure.[146] It further places a series of additional obligations on businesses such as the "purpose limitation" requirement that states that information collected for a purpose cannot then be used for a different one without disclosure, "establish[ing] boundaries around the ways that data controllers may use personal information."[147] It also has provisions requiring deletion or private disclosure of personal information upon request, but this requirement, while robust in principle, is hindered by the "business purpose" exception.[148] Through this exception, a business does not have to honor certain types of requests if it has a valid business reason, defined as an "operational purpose that is compatible with the context in which the personal information was collected."[149]

The issue of limited application of these laws is pervasive, and the FTC has the same sort of conception as laid out in its 2012 Report.[150] The CCPA's exception is easy to exploit because the law

---

[145] Under the CCPA, biometric data ought to be treated and cared for the exact same way as internet browsing history. *See* CAL. CIV. CODE §§ 1798.100(b), 1798.140(o)(1) (West 2022) (grouping biometric data and "electronic network activity" as information in need of equivalent protections).

[146] *See id.* § 1798.130 (describing the required disclosures businesses under the CCPA must give to consumers regarding use of information and data collected).

[147] *See id.* § 1798.100(b) (describing the purpose limitation requirement); Bret Cohen & John Williams, *What Does the CCPA's "Purpose Limitation" Mean for Businesses,* INT'L ASS'N OF PRIV. PROS. (Sept. 29, 2020), https://iapp.org/news/a/what-does-the-ccpas-purpose-limitation-mean-for-businesses; *see also* CAL. CIV. CODE § 1798.100(b) (West 2022) (providing the statutory basis for those limitations on data controllers).

[148] CAL. CIV. CODE § 1798.140(t)(2)(C) (West 2022) (establishing a conjunctive conditions test in order for those data use limitations to apply, directly cabining the statute's scope).

[149] *Id.* § 1798.140(d).

[150] *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICY MAKERS 38 (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommenhe dations/120326privacyreport.pdf (weighing the costs, concerns, and benefits of business purposes being the cornerstone for the application of data privacy laws).

is unclear as to what counts as a business purpose.[151] Interestingly, the fact the law originally called for stricter affirmative opt-in consent protocols would have made the business purpose exception much narrower, but "[a] number of commenters took issue with the attorney general's proposal. They argued that requiring a consumer's opt-in consent for every new purpose discouraged businesses from using customer data in innovative ways and would result in 'notice fatigue.'"[152] Here, deregulation began even before the regulation was born.

And the trend of industry-friendly privacy regulation will continue if U.S. data privacy law continues to focus too narrowly and weakly. For example, commentators have noted the Virginia data privacy law passed in 2021 was watered down by corporate actors and "was very much an industry-led effort by Microsoft and Amazon."[153] Without strong and expressive data privacy regulation, it is simply too easy for deregulators to co-opt the law to their own ends.

Further, most of the law's safeguards relate to security, requiring pseudonymization, de-identification, other technical safeguards, and disclosure where the business sells data to third parties.[154] These are valuable and worthy pursuits, but they do not address privacy itself and do not police what the business who initially collected your data may do with it. For data privacy laws to be effective, privacy cannot take a backseat—it must be expressively advanced as a central value.

Last, CCPA enforcement is limited. The power to enforce lies in the hands of the California Attorney General and the California Privacy Protection Agency who can enforce a maximum $2,500 penalty for unintentional violations and $7,500 for intentional

---

[151] CAL. CIV. CODE § 1798.100(b) (West 2022).

[152] Cohen & Williams, *supra* note 147.

[153] Todd Feathers, *Big Tech Is Pushing States to Pass Privacy Laws, and Yes, You Should Be Suspicious*, THE MARKUP (Apr. 15, 2021, 8:00 AM) (quoting Ashkan Soltani, former Chief Technologist for the Federal Trade Commission), https://themarkup.org/privacy/2021/04/15/big-tech-is-pushing-states-to-pass-privacy-laws-and-yes-you-should-be-suspicious.

[154] *See* Yunge Li, Note, *The California Consumer Privacy Act of 2018: Toughest U.S. Data Privacy Law with Teeth?*, 32 LOY. CONSUMER L. REV. 177, 186–89 (2020) (noting the CCPA's various requirements for data collection).

violations (with enhancements for minors under sixteen).[155] While the law does provide for a private right of action, it is limited to occurrences of a data breach, entrenching the law's commitment to security over privacy.[156]

The GDPR takes a different approach rooted in the European conception of privacy as a human right. For example, the first Recital of the law explicitly states in its first sentence that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right."[157] The Office of the European Data Protection Supervisor correlates this to notions of dignity, explaining that "[p]rivacy is not only an individual right but also a social value."[158] This difference in messaging signals to the public that the European Union looks at them as people, not just consumers.

Further, unlike the CCPA, the GDPR differentiates types of data, designating "special" categories entitled to a greater level of protection than others.[159] This signals that the EU recognizes the human aspect of privacy and endorses the fact that people value certain types of sensitive data more than others, data that warrants maximum. The GDPR otherwise bears similarities to the CCPA by requiring transparency and cybersecurity-related disclosures, along with a right to deletion of personal information upon request.[160] But while the CCPA requires consumers to opt out of data collection, the GDPR creates a list of exclusive legal bases under which data processing is acceptable.[161]

---

[155] *See* CAL. CIV. CODE § 1798.155(b) (West 2022) (setting the penalty ranges according to different levels of violations).

[156] *See id.* § 1798.150 (providing a private right of action for consumers whose data is infiltrated). See CPRA §1798.155, for CPRA's addition of the Privacy Protection Agency and a description of such agency's enforcement authority.

[157] GDPR, *supra* note 4, at 1.

[158] *Data Protection,* OFF. OF THE EUR. DATA PROT. SUPERVISOR (last visited Jan. 17, 2022) https://edps.europa.eu/data-protection/data-protection_en.

[159] Special categories are explained as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation." GDPR, *supra* note 4, at 38.

[160] *See id.* at 43–44 (describing a data subject's rights surrounding erasure).

[161] *See id.*, at 38–39 (listing multiple grounds which data gathering and processing is exempted from the preceding restriction, including explicit consent, performance of contracts,

Regarding enforcement, the GDPR has become somewhat notorious in the realm of fines. The law provides for substantial fines that can hit large companies hard, authorizing fines of up to twenty million euros or four percent of worldwide turnover for the preceding fiscal year, whichever is higher.[162] The largest penalty to date—€746 million[163]—was levied against Amazon for violations by its cookies policy.[164] Fines like this are meaningful and signal that regulators value privacy.

Additionally, the GDPR includes a broader private right of action than the CCPA does.[165] This allows people who have suffered damage as a result of any infringement of the GDPR to sue for compensation, placing the burden on the alleged violator to prove that it is not responsible for the damage.[166] Further, individuals can "lodge a complaint . . . if the data subject considers that the processing of personal data relating to him or her infringes this Regulation."[167]

---

legal compliance, and protection of the vital interest of natural persons, public interest, or legitimate interests that cannot override the fundamental rights of the data subject).

[162] *See id*, at 82–83 ("[S]ubject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.").

[163] *See* Stephanie Bodoni, *Amazon Challenges Record $865 Million EU Data-Protection Fine*, BLOOMBERG (Oct. 15, 2021, 5:05 AM), https://www.bloomberg.com/news/articles/2021-10-15/amazon-fights-record-865-million-eu-data-protection-fine?leadSource=uverify%20wall (reporting on the fine and Amazon's appeal).

[164] *See* Amazon.com, Inc., Quarterly Report (Form 10-Q), at 13 (June 30, 2021) (disclosing the *Commission Nationale pour la Protection des Données's* (CNPD's) decision that "that Amazon's processing of personal data did not comply with the EU General Data Protection Regulation"); *see also* Natasha Lomas, *France Fines Google $120M and Amazon $42M for Dropping Tracking Cookies Without Consent,* TECHCRUNCH (Dec. 10, 2020, 3:55 AM), https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent/ (describing a separate GDPR action, in which Amazon was fined $42 million and Google $120 million for their cookies policies that made opting out unnecessarily onerous, resulting in users simply selecting "agree" to navigate the site, a procedure that was deemed not to satisfy ideas of freely given consent).

[165] *Compare* GDPR, *supra* note 4, at 81 ("*Any* person who has suffered material or non-material damage as a result of an infringement of this Regulation *shall* have the right to receive compensation from the controller or processor for the damage suffered." (emphasis added)), *with* CAL. CIV. CODE § 1798.150 (limiting the private right of action to specific types of injured parties).

[166] *See* GDPR, *supra* note 4, at 81 (granting a "right to receive compensation" unless the controller or processor is "not in any way responsible for the event giving rise to the damage").

[167] *Id.* at 80.

Using this provision, Maximilian Schrems was able to sue Facebook for "coercing" acceptance of data collection policies without meaningful consent.[168] Measures like a private right of action force businesses that would deregulate (and have consistently done so) to comply instead.[169] Fortune 500 companies spent roughly $7.8 billion preparing for GDPR.[170] The GDPR's stringent fines and enforcement have placed privacy in a position of preeminence and increased public awareness of privacy as an issue.[171] Only two years after GDPR went into effect, twenty-nine percent of consumers in one international study switched brands due to data practices, and respondents broadly viewed their national privacy legislation favorably.[172] This comes with a caveat, however. GDPR still focuses on a "rules of the road" approach[173] in which businesses are given too much leeway to avoid the spirit of the law: aspects of GDPR still allow for spontaneous deregulation because the law allows for too much self-regulation. But progress is still happening and norms are being impacted.[174] GDPR, through its expressive stance and its stricter regime, helps shape norms that run counter to the norms that deregulators wish to impose.[175] Privacy is about social norms.[176] If the norm is that people want

---

[168] *See* Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, Case C-311/18, EU:C:2020:559 (July 16, 2020) (detailing the role of the Commission in enforcing Schrems' rights).

[169] *See* Tamar Frankel, *Implied Rights of Action*, 67 VA. L. REV. 553, 556 (1981) (discussing the deterrent effects of implied rights of action).

[170] Anant et al., *supra* note 7.

[171] *See id.* (noting the study's results that reveal increasing consumer awareness of data privacy rights).

[172] CISCO, 2020 CONSUMER PRIVACY SURVEY, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-infographic-2020.pdf.

[173] *See* WALDMAN, *supra* note 37, at 106 (noting that a "regulatory environment where the law on the books states rules of the road" results in "self-regulation under internal consistencies and corporate capture" which is a "gift to the information industry and it is taking full advantage").

[174] *See* Anant et al., *supra* note 7 ("About six in ten consumers in Europe now realize that rules regulate the use of their data within their own countries, an increase from only four in ten in 2015.").

[175] *See supra* notes 157–168 and accompanying text.

[176] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 233 (suggesting that privacy laws should focus on responding to societal needs and expectations). Loose standards in privacy laws allow them to be "co-opted into corporate compliance structures that provide little to no

their privacy to be taken seriously, then it is incumbent on regulators to do so.[177] Not only is this because privacy is so important, but also because, without proper laws, spontaneous deregulation proves that information capitalists will not only circumvent regulation, but will actively attempt to craft new norms.[178]

Overall, American data privacy law is ineffective and a comprehensive and expressive law would do a far better job of protecting privacy rights.[179] The future of data privacy in the U.S. is about discourses, and for privacy-first discourses to win out, the law must be robust and open about the interests it intends to protect. This is because the whole point of expressive law is specifically about creating those very same discourses.[180] Deregulation in this space is too subtle, pervasive, and hostile for data privacy law to do anything less.[181]

C. RECOMMENDATIONS

There is a battle being fought over the norms that will govern data privacy.[182] Spontaneous deregulators are taking advantage and are using regulation itself to craft pro-business norms that benefit them.[183] For example, Apple markets itself very strongly as a privacy champion.[184] Its privacy policy says that "[a]t Apple, we believe strongly in fundamental privacy rights"[185] and elsewhere

---

protection" in real, on-the-ground environments. Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 777 (2020) [hereinafter Waldman, *Privacy Law's False Promise*].

[177] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 75 (explaining that norms and expectations should dictate how regulators behave).

[178] *See id.* at 233 (describing the increasing normalcy of corporations' "performing accountability while exercising great power behind the scenes").

[179] *See infra* section III.A.*5*.

[180] *See supra* note 23 and accompanying text.

[181] *See* Waldman, *Privacy Law's False Promise*, *supra* note 176 (explaining how consumers lose out in absence of regulations).

[182] *See supra* section III.A.

[183] *See supra* section III.A.*4*.

[184] *See Apple Privacy Policy*, APPLE, https://www.apple.com/privacy/en-ww/ (last updated Oct. 27, 2021) (emphasizing Apple's commitment to consumer privacy).

[185] *Id.*

claims that privacy is one of Apple's "core values."[186] However, that does not match actual practices.[187] The iCloud, Apple's backup system that holds many peoples' photos, movies, messages, files, and location data (i.e., a record of their lives), has a back door that Apple holds the encryption keys to.[188] If users do not have a newer operating system, Apple can give all data to Immigrations and Customs Enforcement (ICE) or the police.[189]

Additionally, the company's tools theoretically designed to stop child sexual abuse could also be used to out LGBTQ+ children without their permission.[190] Apple's facial recognition technology shares information with businesses that could create biases against women and people with darker skin.[191] These sorts of consequences are common with deregulators,[192] but with a company the size of Apple, speaking privacy but not practicing it is dangerous.[193] For example:

---

[186] *Privacy*, APPLE, https://www.apple.com/privacy/ (last visited Jan. 22, 2023).

[187] *See* Albert Fox Cahn & Evan Selinger, *Apple's Privacy Mythology Doesn't Match Reality*, WIRED (Aug. 11, 2021), https://wired.com/story/opinion-apples-privacy-mythology-doesnt-match-reality (opining that Apple's commitment to privacy is performative).

[188] *See id.* (discussing how Apple retains iCloud encryption keys, allowing it to access all of a user's backup files at will).

[189] *See id.* ("According to Apple's law enforcement manual, anyone running iOS 7 or earlier is out of luck if they fall into the police or ICE's crosshairs.").

[190] *See* Tiffany C. Li, *Apple's CSAM Prevention Features Are a Privacy Disaster in the Making*, MSNBC (Aug. 12, 2021, 4:42 PM), https://www.msnbc.com/opinion/apple-s-csam-prevention-features-are-privacy-disaster-making-n1276607 (expressing fear that explicit image notifications systems could "potentially out[] LGBTQ children to homophobic families"); Elissa Redmiles, Opinion, *Apple's New Child Safety Technology Might Harm More Kids Than It Helps*, SCI. AM. (Aug. 29, 2021), https://www.scientificamerican.com/article/apples-new-child-safety-technology-might-harm-more-kids-than-it-helps/ (explaining that LGBTQ+ youth are more likely to view images that could be flagged by Apple's content filters, in part due to the lack of effective sexuality education available to them).

[191] *See* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, *in* PROC. OF THE FIRST CONF. ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY 77–91 (Feb. 2018), http://proceedings.mlr.press/v81/buolamwini18a.html.

[192] *See* Edelman & Geradin, *supra* note 10 (explaining how spontaneous deregulation poses dangers to the public).

[193] *See* Cahn & Selinger, *supra* note 187 (explaining the profound negative impact that Apple's actions can have on societal norms, such as accelerated "normalization of both automated ID checks and automated facial scanning").

> Apple's vast penetration of the mobile phone market, the very thing it emphasizes when touting privacy protections, gives it vast power over people's habits. By changing its software, Apple not only changes our behavior, it also subconsciously shifts our beliefs. The adjustment reengineers fundamental aspects of our humanity, like what we expect, desire, and deem socially reasonable.[194]

Apple's practices "are performances, banging us over the head with frequent (albeit dubious) assurances that we can trust tech companies with our data."[195] Like Google's recent remarks on data privacy[196] and Apple's new privacy policy,[197] performative self-regulation can be highly seductive, but it is also easy to manipulate by deregulators. For example, when faced with disclosure rules about cookies, many websites today will present the user with a popup that asks them if they want to accept cookies.[198] If users wish

---

[194] *Id.*

[195] WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 75.

[196] *See Google's Sundar Pichai: Excerpts from a Conversation at the WSJ's Tech Live Conference,* WALL ST. J. (Oct. 21, 2021, 4:22 PM) https://www.wsj.com/articles/googles-sundar-pichai-excerpts-from-a-conversation-at-the-wsjs-tech-live-conference-11634847777 (discussing Google's new data privacy and using data for advertisements). At the conference, Alphabet Chief Executive Officer Sundar Pichai pushed for "global frameworks," but primarily as they relate to cybersecurity, not to privacy as a value. *Id.*

[197] *See* Patience Higgins & Suzanne Vranica, *Apple's Privacy Change Is Hitting Tech and E-Commerce Companies. Here's Why*, WALL ST. J. (Oct. 22, 2021), https://www.wsj.com/articles/apples-privacy-change-is-hitting-tech-and-e-commerce-companies-11634901357 (explaining how "Apple's new policy requires apps to ask users if they want to be tracked"); *see also* Brian X. Chen, *The Battle for Digital Privacy Is Reshaping the Internet*, N.Y. TIMES (Sept. 21, 2021), https://www.nytimes.com/2021/09/16/technology/digital-privacy.html (providing more perspectives on the impacts of Apple's privacy policy changes, and noting that "[s]ince Apple released the pop-up window, 80 percent of iPhone users have opted out of tracking worldwide"). But Apple's own advertising is entirely unaffected by the restrictions its privacy policy imposes on other firms. *See* Rachel Kraus, *The Result of Apple's New Privacy Policy? More Money for Apple*, MASHABLE (Oct. 17, 2021), https://mashable.com/article/apple-privacy-policy-advertising-increase (noting how Apple does not rely on advertising for most of its revenue and may be using purportedly pro-privacy tools to undermine competition instead).

[198] *See What Percentage of Websites Utilize a Banner That Seeks Opt-in Consent Before Deploying Cookies?*, BRYAN CAVE LEIGHTON PAISNER (Mar. 6, 2020), https://www.bclplaw.com/en-US/insights/what-percentage-of-websites-utilize-a-banner-that-

to opt out, however, they face complex settings screens that can be daunting, difficult, and time-consuming.[199] Most users simply do not bother.[200] Moreover, self-regulation carries absolutely no accountability. Amazon, for example, repeatedly touts that consumer trust is its "highest priority," and yet consistently fails to protect its customers from bad actors while minimizing privacy concerns internally.[201]

This is an excellent example of deregulators innovating around laws that they do not like, creating empty performances in the place of regulation. Additionally, when Target executed its pregnancy advertising scheme,[202] the company technically violated no privacy law. When JetBlue violated user privacy by intentionally violating its own privacy policy, it technically violated no law.[203]

GDPR fines[204] demonstrate that tides may be changing, but not enough and not in the United States.[205] Trusting information capitalists (who are profit motivated to collect as much information as possible) to police themselves is a conflict of interest regulation ought to address.[206] Otherwise, spontaneous deregulation allows

---

seeks-opt-in-consent-before-deploying-cookies.html (explaining that about 10.6% of Fortune 500 companies deployed a "notice + opt-in consent" cookie banner in 2020).

[199] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 132 ("Many . . . laws require that privacy policies be sufficiently 'conspicuous' to users, and yet privacy policies today are confusing messes of legalese jargon and vague marketing platitudes that . . . don't actually provide notice.").

[200] *See* Auxier et al., *supra* note 50 (noting that only "9% of adults say they always read a company's privacy policy before agreeing to the terms and conditions").

[201] *See* Will Evans, *Amazon's Dark Secret: It Has Failed to Protect Your Data*, WIRED (Nov. 18, 2021, 6:00 AM), https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/ (detailing numerous failures within the company to safeguard customer data, including from Amazon's own employees). A former Amazon lawyer even stated that the company's rhetoric on privacy was "simply inaccurate." *Id.*

[202] *See supra* note 131 and accompanying text.

[203] *See supra* note 19 and accompanying text.

[204] *See supra* notes 162–164 and accompanying text.

[205] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 240 ("[W]ithout more, privacy regulation from the FTC . . . and technology companies will remain the primary movers in determining what a given legal standard requires.").

[206] *See id.* at 233 ("Many companies in the information industry have perfected the art of performing accountability while exercising great power behind the scenes, clearing away the discursive, legal, and procedural obstacles to extracting our data. . . . From a law and political economy perspective, law has a role to play as an explicit counterweight to information industry power.").

Big Tech to fashion data privacy rules in its own image without consequence and renders the law out of sync with genuine societal values.[207] Companies release new features and products multiple times a year[208] that threaten to circumvent existing laws that hew too closely to tech specificity.

To move forward, "[w]e need new privacy performances."[209] In the United States, performances need to focus on respecting privacy as a fundamental right because "[a]ctions are expressive; they carry meanings."[210] And the law should use this sense of expression to protect privacy as a social norm, not as a commercial interest.

1. Data Privacy as a Right in Itself. Too many American data privacy laws are narrowly focused on specific industries and commercial concerns,[211] rendering them susceptible to circumvention or co-option by deregulators. Ensuring that the law is expressively designed to protect data privacy itself as an interest with direct and unambiguous language will help to curb and avoid issues like the *JetBlue* case[212] and insulate against the ever-evolving nature of technology. And the language must go beyond nice phrases in preambles.[213] The text of the law throughout must be, first and foremost, centrally about privacy, not as a companion to any other value. Laws that are directly about privacy would be harder to avoid. Therefore, the law's functional focus should be the protection of people and their privacy interests.

2. Personal Liability. The SEC currently requires officers of publicly traded companies to sign off on their annual reports, with personal liability for fraud attaching.[214] Framing American privacy

---

[207] *See* Edelman & Geradin, *supra* note 10 ("A common defense [asserted by spontaneous deregulators'] is to claim that consumers can dispense with traditional protections because the platform offers an alternative, possible superior protection mechanism.").

[208] *See, e.g.*, Adam Burakowski, *Understanding the Product Cycle: When to Expect New Releases, Updates, Deals, and Discounts*, N.Y. TIMES: WIRECUTTER (Jun. 10, 2016), https://www.nytimes.com/wirecutter/blog/understanding-the-product-cycle-when-to-expect-new-releases-updates-deals-and-discounts/ (reviewing how and when technology companies release new products).

[209] WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 233.

[210] Sunstein, *supra* note 23, at 2021.

[211] *See supra* notes 80, 141 and accompanying text.

[212] *See supra* notes 17–20 and accompanying text.

[213] *See supra* note 157 and accompanying text.

[214] *See* 17 C.F.R. § 228 (establishing the duty requiring issuers to maintain and "evaluate the effectiveness of" their disclosures or risk liability).

law to place a similar duty on companies regarding their privacy policies and holding corporate officers personally liable for privacy violations creates higher stakes and sends messages about seriousness because it attaches a risk that is specific to the individuals who can address the privacy harm in the first place.

3. A Private Right of Action. An unqualified private right of action that would allow individuals to sue for violations of their privacy rights is a critical expressive component of an effective data privacy law. If the norms we want to promote involve individual rights, it is only sensible that the law allow individuals to take charge of their own rights. Without it, people would depend on state actors, a risky proposition given that the populations most in need of privacy protection are the populations that, historically, state action has failed the most.[215]

4. Fines. The adage "money talks" is applicable here—fines are the most publicized and visible components of data privacy laws.[216] They demonstrate that the law takes violations seriously and have the expressive, norm-setting effect of altering corporate behavior to avoid such sanctions. They also speak a language that businesses understand: by penalizing behavior with the very thing that businesses stand to gain from engaging in such behavior, fines remove the incentive. Further, fines provide notice that such behavior comes at a cost.

5. Opt-In Consent. The CCPA and other American privacy laws generally operate on an opt-out consent model, meaning that it is incumbent on the individual to tell companies not to use their data.[217] An opt-in model would shift that burden to the company to ask the individual before it collects data and allow the user to choose whether to accept certain features that collect personal data. This expressive gesture would shift power from deregulators to individuals.

6. Lessons from GDPR. The GDPR's comprehensiveness, aggressive language, system of fines, and private right of action all

---

[215] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 237 (noting that "traditionally marginalized groups . . . bear an unequal burden of information age harms" and arguing that "public regulation of the information industry" is important to counteract discourses within a process that has "for too long immunized itself from public accountability").

[216] *See supra* notes 162–164 and accompanying text.

[217] *See supra* note 152 and accompanying text.

represent positive steps towards protecting privacy. The U.S. should adopt a similar approach because data does not have borders,[218] and therefore, privacy does not either. Again, this is not to say that the GDPR is perfect.[219] The GDPR could go much further by enforcing things like data minimization,[220] a value expressed in the Regulation but not enforced often enough.[221] Enforcement is one of the key strategic responses advanced in order to curtail spontaneous deregulation of Big Tech[222] and it could transform what appear to be guidelines in the statute into genuine bans on untoward conduct.

7. Progressive Regulation. Another option would be to follow a proposal like Ohio Senator Sherrod Brown's Data Accountability and Privacy Act that would imbue data privacy with the flavor of civil rights by prohibiting discriminatory data collection and usage.[223] This is key to stopping spontaneous deregulation as a significant risk factor of that phenomenon is discrimination,[224] and progressive regulation recognizes the power of the expressive function of law to entrench and alter norms and use that to counterbalance the discord caused by the counter-democratic norms emphasized by deregulators.

---

[218] *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) ("Global computer-based communications cut across territorial borders, creating a new realm of human activity and undermining the feasibility—and legitimacy—of laws based on geographic boundaries.").

[219] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 248 ("[T]he GDPR lays out 'rules of the road' for corporate data collection and processing even though it is framed as an approach based on fundamental human rights.").

[220] Data minimization refers to a process by which a company does not collect more data on a user than it absolutely needs. GDPR, *supra* note 4, at 35.

[221] *See* Natasha Lomas, *Big Changes Coming for GDPR Enforcement on Big Tech in Europe?*, TECHCRUNCH (Jan. 31, 2023, 11:25 AM), https://techcrunch.com/2023/01/31/gdpr-enforcement-reform-dpa-oversight/ (arguing that adequate enforcement of GDPR is "long overdue" and subject to "long standing criticism").

[222] *See* Matt Burgess, *How GDPR Is Failing*, WIRED (May 23, 2022, 7:00 AM), https://www.wired.com/story/gdpr-2022/ (reporting on recent GDPR enforcement actions and their "incalculable effect on data practices broadly").

[223] *See* Data Accountability and Transparency Act of 2020, S. 116th Cong. § 3(19)(E) (2020) (explicitly identifying discrimination as a cognizable privacy harm).

[224] *See* Edelman & Geradin, *supra* note 10 (noting that "it is unclear whether or how this requirement [requiring equal treatment] applies to less-regulated platforms").

D. ADDRESSING SOME COUNTERARGUMENTS

Proponents of deregulation, sectoral regulation, and corporate power push the values of innovation and efficiency.[225] But framing the argument in these terms marginalizes privacy in unacceptable ways[226] and creates a false narrative that the concepts of innovation and privacy are diametrically opposed.[227] These normative arguments play precisely into the risk factors of spontaneous deregulation[228] and the importance of privacy in modern society necessitates an expressive performance on the part of regulation to stop it.

Others have pushed back against some of the GDPR's mechanisms, predominantly its structure of fines, arguing, simply, that they do not work.[229] Companies nearly always appeal their fines and have successfully done so at an alarming rate.[230] This may give the impression that the fines do nothing, but that position overlooks two important points. First, The fines do serve an expressive function of outing industry actors for their privacy

---

[225] *See supra* notes 112–115 and accompanying text.

[226] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 65 ("Innovation, industry says, is always a normative good . . . [t]he information industry argues that if we want a world where entrepreneurs are building . . . whatever the next 'big thing' will be, then law not only has to facilitate innovation, it has to stand aside."). While industry actors tend to be publicly pro-regulation, they also "have testified before Congress to argue that privacy law will stifle progress." *Id.*

[227] *See* Cohen, *What Privacy Is For*, *supra* note 117, at 1905 (arguing that "[p]rivacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable," and is thus actually a boon to innovation.)

[228] *See* Edelman & Geradin, *supra* note 10 ("Caught up, perhaps, by enthusiasm for their model ad a belief in its utility for customers, the founders and managers of these companies seem to see many of the existing rules as unwanted holdovers from a bygone era not yet ready for their innovations.").

[229] *See* Burgess, *supra* note 222 ("[B]ut four years after GDPR started, the total number of major decisions against the world's most powerful data companies remains agonizingly low.").

[230] *See* Catherine Stupp, *Wave of Legal Appeals Challenges How European Regulators Enforce Privacy Rules,* WALL ST. J. (Mar. 15, 2021, 5:30 AM), https://www.wsj.com/articles/wave-of-legal-appeals-challenges-how-european-regulators-enforce-privacy-rules-11615800602 ("European courts struck down or reduced several multimillion-dollar fines in recent months . . . [and] [c]ompanies taking note are more willing to challenge authorities' rulings.").

violations in very public ways.[231] Googling "GDPR fines" will reveal dozens of results about Amazon, Facebook, or WhatsApp.[232] And second, the fines are not being overturned on substantive grounds, but rather due to procedural errors.[233] This is unfortunate, but it is important to note that the GDPR system is only three years old and European authorities have never tried to enforce it before. Procedural errors say nothing about the actual impact of the levying of the fine and the substantive basis for the fine remains.

On the opposite end of the spectrum, scholars have suggested that the GDPR does not go far enough and that more advanced pro-privacy measures should be put in place.[234] Many proposed changes to privacy law, such as private rights of action, "would not be able to bring about real change for privacy on the ground."[235] Suggestions such as increased representation for marginalized populations who are historically disproportionately victimized by privacy violations and the creation of technology research unions are all good ideas.[236]

While these proposals place privacy above corporate concerns and treat it as importantly as it ought to be, they fail to recognize the difficulties of passing new privacy legislation.[237] It is unclear how any of these more advanced measures would actually be achieved. Deregulators are also likely to fight tooth and nail against any advance because they have too much money in the game. $150 billion of Google's revenue comes from advertising,[238] and Facebook

---

[231] *See supra* notes 162–164 and accompanying text.

[232] *See, e.g.,* Katie Collins, *GDPR Fines: The Biggest Privacy Penalties Handed Out So Far*, CNET (Feb. 21, 2022, 5:00 AM), https://www.cnet.com/tech/gdpr-fines-the-biggest-privacy-penalties-handed-out-so-far/ (reporting on a range of the largest such fines).

[233] *See* Stupp, *supra* note 230 (noting that in one such case, a German company's $17.3 million fine was overturned because the regulator did not identify the individual employee responsible for the violation).

[234] *See* WALDMAN, INDUSTRY UNBOUND, *supra* note 37, at 237 (arguing that "traditional approaches to privacy law have left a lot of people behind").

[235] *Id.* at 238.

[236] *See id.* at 242–44 (recommending each of these approaches in turn).

[237] *See* Rebecca Kern, *Bipartisan Draft Bill Breaks Stalemate on Federal Data Privacy Negotiations*, POLITICO (Jun. 3, 2022, 1:17 PM), https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092 (noting that "Congress has tried and failed for decades to pass a law to protect Americans' data privacy").

[238] Megan Graham & Jennifer Elias, *How Google's $150 billion advertising business works,* CNBC (May 18, 2021, 12:52 PM), https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html.

makes $25.44 billion a year on the practice.[239] Apple does not work this way, and when the company implemented its decision to internalize its advertising and push consent across its App Store, Facebook argued that the decision would impact thousands of other businesses,[240] and while their motivation may have been nefarious, the fact is concerning. Because the digital environment moves so fast and because there are conflicting norms so heavily at odds with each other, every action taken has consequences that impact more than just the people that they target.

Privacy has also become political, complicating the issue further.[241] The unfortunate reality is that we are so far behind on regulation that industry leaders and deregulators have been able to build empires off consumer data. Those empires have people living in them, meaning there must be an actionable plan in place with proposals that have genuine steps and end goals. It is valid to desire an outcome, but taking positive steps along the way to achieve that outcome and then planning for it in a way that can succeed is still valuable. This is not to say that the battle is won—far from it. But privacy discourses have changed, some for the worse, clearly, but also some for the better, and that is worth building on so long as we remain conscious of the pro-corporate norm-creators who will constantly act against the interests of privacy as an actionable human right.

IV. CONCLUSION

In 1890, Louis Brandeis and Samuel Warren warned that advancing technology and privacy are naturally predisposed to conflict—they urged that privacy law be adaptable and flexible in order to meet the challenge.[242] Brandeis was speaking of the advent

---

[239] Sarah E. Needleman, *Facebook's Ad Business Drives Surge in Revenue, Following Google's Act*, WALL ST. J. (Apr. 28, 2021, 7:00 PM), https://www.wsj.com/articles/facebook-fb-1q-earnings-report-2021-11619610405.

[240] *See* Chen, *supra* note 197 (noting the tension between Facebook, Apple, and the small businesses being caught in the middle).

[241] *See* EY GLOBAL, *supra* note 7, at 29 ("Consumer data privacy is an established partisan issue in the US.").

[242] *See* Warren & Brandeis, *supra* note 36, at 196 ("Of the desirability—indeed of the necessity—of some such protection [in the face of new technology], there can, it is believed,

of portable photography, faster communications, and a Gilded Age tabloid-centric press environment.[243] But with technology now advancing faster than could have been anticipated, we must take privacy law seriously. Spontaneous deregulation allows companies that use tech aggressively and perniciously to achieve profit-maximizing ends prey on vulnerable individuals.

That modern technology has allowed personal integrity to be leveraged for profit brings Brandeis's concerns into an unprecedented forum. Spontaneous deregulators are dangerous because they subvert genuine democratic norms and replace them with pro-business norms. This is unacceptable—law's expressive function should be used to reset those norms and push back against information capitalism to preserve the dignity of actual people, especially in an environment where it is easy to slip into complacency with an unnecessary, dangerous, and anti-democratic regime that seeks to avoid regulation. By pushing back steadily, people and regulators can and must entrench norms that privacy is a human right—not merely an empty shell of a right, but an actionable one with consequences for infringement upon it.

Privacy is a slippery concept. Some say it is "impossible to protect" in a world where state actors, small businesses, and large multinational corporations alike "gather unprecedented amounts of personal information on their users."[244] But it is precisely because of this pervasive system wherein major industry actors require and use so much personal information that there ought to be a comprehensive, thoughtful approach to the responsible treatment of that information. This Note urges that, while privacy is difficult, it is not impossible at all.

---

be no doubt."); *see, e.g.*, *id.* at 200 (opining on the poor applicability to privacy of traditional property rights).

[243] *See id.* ("Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.").

[244] GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES 3 (2014).