Comment

NOAH ASHMAN*

Outed by Advertisements: How LGBTQ Internet Users Present a Case for Federal Data Privacy Legislation

* J.D. Candidate, 2021, University of Oregon School of Law; Editor in Chief, *Oregon Law Review*, 2020–21; B.S., 2018, University of California, Los Angeles. Thank you to Professor Suzanne Rowe, whose guidance and words of encouragement set this Comment in motion. Thank you to the friends and peers who helped keep this Comment on track with Sunday night phone calls and library pep talks. Finally, thank you to the staff of *Oregon Law Review* for the support and feedback throughout this process.

INTRODUCTION

I was sitting on a bus when I first noticed a recurring phenomenon in my life: social media's ability to out me as LGBTQ in public spaces. I had just moved away from Los Angeles and started to get my bearings in a new, much smaller city. I was on a crowded bus with my backpack in my lap, headphones in my ears, and my phone in my hand as I somewhat mindlessly scrolled through Twitter to entertain myself on the thirty-minute ride home from school. During those thirty minutes, I probably read some *L.A. Times* news story about home, liked some celebrity's post, and retweeted something that made me laugh. But I had not stopped to think about how my internet use had already caused the inanimate piece of technology in my hand to identify me as LGBTQ. All the evidence was there for the algorithms to work their magic. I followed LGBTQ media sites like The Advocate and NewNowNext, and I even followed a few drag queens for some extra entertainment. For my phone, which was indubitably smarter than I, it was a no-brainer.

Because my phone identified me as LGBTQ, however, a targeted advertisement interrupted my mindless scrolling. The advertisement was for an LGBTQ dating app I had no intention of downloading, and it included an image with just a bit more intimacy than I am comfortable seeing on a crowded bus. I quickly scrolled past the advertisement, but I became much more aware of the space I was occupying. I looked behind me. I looked next to me. I thought about who might have seen what was on my screen, and I started preparing what I would say if someone made a comment. I started preparing what I would do if the situation escalated beyond just a comment.

Luckily, no conflict actually arose in this situation. As it turned out, the tired bus riders around me were not paying attention to the advertisements I was receiving between tweets from the Governor and my roommate from college. Nonetheless, this scenario opened my eyes to what I soon discovered to be a fairly common phenomenon. Within a few weeks, I received a text message from a close friend, thousands of miles away, who worried about whether the woman behind him on a commuter train had noticed a similar advertisement on his screen.

Shortly thereafter, a classmate complained about seeing a suggested post for an article titled "Ten Celebrities You Didn't Know Were LGBTQ" when her attention moved from textbook to Facebook at the library.

While these examples initially appear to be inconveniences more than safety concerns when taken at face value, LGBTQ individuals do not always have the fortune of being safely out in public spaces—and the story does not always end with physical safety. The danger of being "outed" in a nation that lacks federal protection for sexual orientation and gender identity implicates numerous possibilities for discrimination. LGBTQ people still risk being fired from their jobs or denied housing if too much of their personal information is revealed.[1] This reality gives much greater magnitude to the fact that an LGBTQ-targeted advertisement can creep its way into social media and reveal too much about a person's life in the wrong setting. Thus, without statutory protections for personal data, the potential consequences for LGBTQ internet users continue to stew.

This Comment addresses the phenomenon of "outing" for the LGBTQ community through the lens of online data storage and argues that a more uniform data privacy scheme is necessary to mitigate the problem. Part I discusses "right of privacy" jurisprudence in federal courts and provides information about the segmented ways data is currently protected. Part I then uses that foundational information to identify a gap in United States data privacy—a gap that leaves the LGBTQ community vulnerable. Part II walks through features of other data privacy schemes, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Part III explores LGBTQ internet use and emphasizes the importance of LGBTQ privacy online.

Finally, Part IV calls for federal legislation to increase protections over personal data and standardize data privacy in the United States.

---

[1] Although the Supreme Court extended Title VII employment discrimination protections to cover gender identity and sexual orientation in *Bostock v. Clayton County*, 140 S. Ct. 1731 (2020), it remains unclear how religious exemptions may interfere. Jon Webb, *Despite Supreme Court Ruling, You Can Still Get Fired for Being Gay, Transgender*, COURIER & PRESS (June 16, 2020, 9:20 AM), https://www.courierpress.com/story/opinion/columnists/jon-webb/2020/06/16/despite-supreme-court-you-can-still-get-fired-being-gay-trans/3197494001/ [https://perma.cc/AJG5-JDJD]; *see also* Lou Chibbaro Jr., *Study Reveals LGBT Rental Housing Discrimination*, WASH. BLADE (July 23, 2017, 9:10 AM), https://www.washingtonblade.com/2017/07/03/lgbt-rental-housing-discrimination/ [https://perma.cc/Y5N2-GCPU].

Part IV also acknowledges and rebuts some lingering concerns with expansive data privacy, such as difficulties finding infringers in the field of intellectual property and general feasibility. The Comment ultimately concludes that federal data privacy legislation is a necessity.

I
BACKGROUND ON PRIVACY

A. The "Right of Privacy" in the United States

Intuitively, personal privacy is extremely important—so important, in fact, that the United States recognizes it as a constitutional right.[2] Consequently, when citizens must disclose pieces of personal information to the government, our case law tells us the government must protect that information with robust systems to avoid infringing the right of privacy.[3] But what about when our information exists outside these robust systems? And what about when our information is held by private companies, rather than by the government? The cell phones we all keep in our pockets, for example, contain more information about us than we realize, and the average citizen does not always know what is done with our information in the ethereal space we call the "cloud."[4] This creates a large question about how a *lack* of a data privacy system may implicate personal privacy concerns. This question becomes particularly concerning when considered with the fact that intimate details like sexual orientation may be compromised by a lack of adequate data privacy protections. Consequently, these concerns with personal devices' capabilities and the intimate details they store collectively compel a more standardized system of data privacy for United States residents.

When it comes to data held by government entities, the United States Supreme Court has long recognized the right of privacy for citizens.[5] In its landmark decision in *Griswold v. Connecticut*, the Court found that the right of privacy is woven into the Constitution, and held that the penumbras of the First, Third, Fourth, Fifth, and Ninth Amendments collectively breathe life into a privacy right "older than

---

2 Griswold v. Connecticut, 381 U.S. 479, 484–85 (1965).

3 Whalen v. Roe, 429 U.S. 589, 606 (1977).

4 *See* Joe McKendrick, *Most Americans Don't Understand Cloud Computing: Does It Really Matter?*, FORBES (Aug. 29, 2012, 9:54 AM), https://www.forbes.com/sites/joemckendrick/2012/08/29/most-americans-dont-understand-cloud-computing-does-it-really-matter/?sh=39d477044ef7 [https://perma.cc/T2AR-ZM6Y].

5 *Griswold*, 381 U.S. at 484–85.

the Bill of Rights" itself.[6] The bounds of this right were not clearly drawn at the time, but the Court later suggested in *Whalen v. Roe* that the right of privacy is broad and covers both the interest in personal matters remaining undisclosed and the interest in making important decisions independently.[7]

In *Whalen*, a New York statute was challenged under both protected privacy interests.[8] The statute required doctors who prescribed certain legal drugs to file a form with the state that included patients' names, addresses, and ages.[9] The challengers alleged that the statute created a potential for disclosure of personal information and discouraged patients from choosing to accept prescriptions.[10] The Court ultimately held that no privacy rights were invaded,[11] but the Court did highlight the fact that collection and storage of data must generally be paired with security provisions and duties to avoid unwarranted disclosures.[12] Thus, a defined, secure system for storing citizens' information would appropriately protect the right of privacy as it pertains to government action. With this in mind, however, there is still a unique concern regarding the power that private actors hold as they collect and store the intimate details we reveal on our personal devices.

Supreme Court Justices have acknowledged the uniqueness of data stored on personal devices.[13] Chief Justice John Roberts has drawn special attention to cell phone storage capabilities, for example, and has drawn attention to how much our phones reveal about our personal lives.[14] Private information, such as addresses, bank information, and photographs, is frequently found in cell phones—all with stamps of time, date, and location to string together a person's precise story.[15] Additionally, Justice Sonia Sotomayor has expressed fear that personal freedoms can be restricted by the knowledge that the "government may be watching"[16] and has cautioned that intimate details like sexual associations may be inappropriately discovered and abused using the

6 *Id.* at 484, 486.

7 *Whalen*, 429 U.S. at 599–600.

8 *Id.* at 599.

9 *Id.* at 592.

10 *Id.* at 600.

11 *Id.*

12 *Id.* at 606.

13 *See, e.g.*, Riley v. California, 573 U.S. 373, 393 (2014).

14 *Id.* at 394.

15 *Id.*

16 United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

information stored in cell phones.[17] While these opinions from the Justices again address the protection of privacy only as it relates to government action, the sentiments, nonetheless, carry weight in the realm of general privacy in the digital age. If the Justices of our highest court are so concerned with the damage that can be done to citizens when the government uses their personal data, it seems to follow that United States residents deserve greater protections overall.

Other federal courts have held that sexual orientation, specifically, falls within the "zone of privacy" to be protected.[18] In *Sterling v. Borough of Minersville*, the Third Circuit held that a teenage boy's right of privacy was violated[19] when a police officer threatened to disclose the boy's sexual orientation to his grandfather if the boy did not do so on his own.[20] The fear of being outed ultimately led the boy to die by suicide, and his mother filed suit alleging that the officer's threat of disclosure violated her son's right of privacy under the Fourteenth Amendment.[21] In response, the Third Circuit recognized that information about sexuality should be "carefully guard[ed]."[22] Finding it difficult to picture anything more private than sexuality, the court suggested that a legitimate government disclosure of a person's sexual identity would be rare.[23]

Although *Sterling* did not specifically involve a disclosure flowing from stored personal data, the court's remarks demonstrate that sexual identity is a highly sensitive matter worthy of protection under the law. Viewing this concern in tandem with the Supreme Court's caution regarding data storage on personal devices, there is a compelling reason to standardize data privacy law to provide uniform protection over intimate details such as sexual orientation, whether or not that information lies in the hands of the government or private actors. But

---

17 *See id.* at 415–16.

18 *E.g.*, Sterling v. Borough of Minersville, 232 F.3d 190, 196 (3d Cir. 2000).

19 *Id.* at 198.

20 *Id.* at 193. The police officer found the teenage boy sitting in his car with a male friend. *Id.* at 192. Suspicious that the boys had been drinking alcohol, the officer searched the car and discovered two condoms. *Id.* The officer then questioned the boys about whether they were in the car together for sexual purposes, and the boys confirmed that they were. *Id.* The boys were ultimately arrested for underage drinking, but the officer separately "counseled [them] against homosexual activity" and threatened to disclose their relationship. *Id.* at 192–93.

21 *Id.*

22 *Id.* at 196.

23 *Id.*

still, the United States does not have a statutory scheme for data privacy.

B. The Futility of Existing Data Privacy Protections

In the absence of a uniform data privacy scheme, the United States has only loose opportunities available to address data privacy concerns. These opportunities can be considered in three categories. First, the Federal Trade Commission (FTC) has stepped into the role of policing consumer privacy and data security.[24] The FTC's role, however, is still very limited, and the scope of the FTC's authority has unclear bounds.[25] Second, nonprofit organizations such as the Network Advertising Initiative (NAI) have provided privacy guidelines for technology providers, but these organizations allow very little room for direct consumer remedy and still pose problems. Third, some federal statutes touch on data privacy and protect very specific industries,[26] but these statutes do not provide United States citizens any generic protections over their data.

1. The Role of the FTC

As industries have rapidly embraced the capabilities of the internet, the FTC has arisen as the primary entity for policing consumer privacy and security.[27] The FTC's authority is only implied, however, as there is no express provision regarding data in the agency's enabling statute.[28] The statute only provides the FTC authority to prevent the use of "unfair methods of competition . . . and unfair or deceptive acts or practices" that have an effect on commerce.[29] Consequently, the FTC is only able to regulate data privacy in instances where the use of consumer data is part of deceptive or unfair business practices.[30] Because data privacy concerns can extend beyond just deceptive or unfair uses of consumer data, the FTC's authority regarding data

---

24 Julia Whall, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of* LabMD, 60 B.C. L. REV. ELEC. SUPP. II.-149, II.-153 (2019).

25 *See id.* at II.-160.

26 Evan M. Wooten, *The State of Data-Breach Litigation and Enforcement: Before the 2013 Mega Breaches and Beyond*, 24 COMPETITION 229, 230 (2015).

27 Whall, *supra* note 24, at II.-153.

28 *See* 15 U.S.C. § 45.

29 *Id.* § 45(a)(2).

30 Whall, *supra* note 24, at II.-154.

privacy is limited. Furthermore, the scope of the FTC's authority remains unclear.

The FTC has settled nearly all its actions against companies that have breached consumer data security.[31] As a result, the agency has not promulgated any rules,[32] nor has the agency's authority been clarified significantly through case law. In a Third Circuit case, for example, the court declined to analyze the FTC's interpretation of its own authority in the context of data security.[33] Rather, the Third Circuit resolved the issue by deciding whether a company's conduct could be considered "unfair" under the language of the statute despite the FTC's interpretation.[34]

Another case, recently decided in the Eleventh Circuit, arguably muddied the FTC's role in the realm of data privacy.[35] The Eleventh Circuit did little to clarify what authority the FTC actually holds, yet the court criticized the "reasonableness" standard the FTC had been using to determine what constitutes an unfair business practice.[36] More specifically, the Eleventh Circuit suggested that the FTC must identify which acts are unfair within a data security program rather than deem the program wholly unfair.[37] After this case, the FTC has little guidance on how to regulate data practices, and private companies have little guidance on how to comply.[38] Thus, the efforts to regulate data privacy at the federal level are insufficient and likely create more confusion than protection for consumers.

Despite the murky nature of the FTC's authority, the agency has consistently displayed interest in clarifying consumer data rights.[39] The

---

31 Wooten, *supra* note 26, at 236.

32 *Id.*

33 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 253–54 (3d Cir. 2015).

34 *Id.* at 255.

35 *See* LabMD, Inc. v. FTC (*LabMD III*), 894 F.3d 1221 (11th Cir. 2018); Whall, *supra* note 24, at II.-164.

36 *See LabMD III*, 894 F.3d at 1235–36.

37 *See id.* at 1237.

38 Julia B. Jacobson et al., *Be Reasonable: Recent FTC Enforcement Orders on Data Security*, LAW.COM (June 24, 2020, 7:00 AM), https://www.law.com/legaltechnews/2020/06/24/how-to-be-reasonable-recent-ftc-enforcement-orders-on-data-security/?slreturn=20201014013246 [https://perma.cc/4HF3-ZTND] ("Despite this relatively long history of data security activity, the FTC is criticized for insufficiently clear guidance about what reasonable data security means, including by the 11th Circuit, which vacated a 2016 FTC data security mandating 'a complete overhaul of LabMD's data-security program' because it offered 'precious little about how this is to be accomplished.'").

39 FED. TRADE COMM'N, FTC STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING, at i (Feb. 2009) [hereinafter FTC STAFF REPORT], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff

FTC held a series of public hearings in 2006 to prepare for potential consumer privacy issues as technology continued to develop.[40] Following these hearings, the FTC began to focus significantly on concerns with online behavioral advertising, or "the practice of tracking consumers' activities online to target advertising."[41] This practice, familiar to most internet users, is what causes an LGBTQ-targeted advertisement to manifest on social media—whether or not it is actually desired.

To respond to specific concerns about online behavioral advertisements, the FTC held town halls and welcomed public commentary to develop a set of self-regulatory principles for online advertisers.[42] The agency ultimately developed four principles for online advertisers to follow: transparency, reasonable security and limited retention of data, express consumer consent to make material changes to privacy policies, and express consumer consent to use sensitive data.[43] These principles aim to balance the benefits of behavioral advertising with the importance of consumer privacy and control.[44] It is important to note, however, that these principles—as well as other reports and guidelines produced by the FTC—only provide a "soft" legal basis.[45] The principles may nudge online advertisers to adjust their practices, but that does not mean they are mandatory or provide a remedy when they are not followed.[46] So while the FTC may recognize that sensitive information like sexual orientation should be protected,[47] recognition alone cannot prevent improper use of sensitive information, nor does it allow a citizen to seek remedy from the entity misusing the information.

-report-self-regulatory-principles-online-behavioral-dvertising/p085400behavadreport.pdf. [https://perma.cc/Q42J-UFRL].

40 FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 1 (2007), https://www.ftc.gov/sites/default/files/documents/public_statements/online-behavioral-advertising-moving-discussion-forward-possible-self-regulatory-principles/p859900stmt.pdf. [https://perma.cc/E6X3-42NU].

41 *Id.*

42 FTC STAFF REPORT, *supra* note 39, at i–ii.

43 *Id.* at 46–47.

44 *Id.* at ii.

45 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 625 (2014).

46 *See id.* at 626.

47 FTC STAFF REPORT, *supra* note 39, at 23.

2. The Role of the NAI

The realm of online behavioral advertising is also led by the Network Advertising Initiative (NAI), a nonprofit organization dedicated to collecting and using data responsibly.[48] The NAI is a self-regulatory organization consisting of more than one hundred member companies,[49] including Google and Microsoft.[50] Since 2000, NAI member companies have collaborated to create and update a code of conduct that each company must follow to ensure that user data is treated uniformly.[51]

The current NAI Code of Conduct outlines a number of requirements for its members.[52] For example, NAI members must give "clear, meaningful, and prominent notice" to users regarding the way data is collected, transferred, and used for tailored advertising.[53] Additionally, NAI members are required to make reasonable efforts to educate users on the choices they have available regarding tailored advertising,[54] with the choices varying based on the amount of sensitive data involved.[55] Notably, the NAI treats information about users' sexual orientation as sensitive,[56] and the Code of Conduct requires opt-in consent from users to collect or store information about actual or perceived LGBTQ status.[57] Although these requirements demonstrate an admirable concern for user privacy, two general problems still persist with data collection and use. First, a large disconnect still exists between users and advertisers due to the complexity of privacy policies, which can make consent ineffective when it is required. Second, the NAI's self-regulatory nature may be insufficient for holding companies

---

48 *About the NAI*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/about-nai/about-nai [https://perma.cc/Z9LG-56HK].

49 *Id.*

50 *NAI Members*, NETWORK ADVERT. INITIATIVE, https://www.networkadvertising.org/participating-networks/?page=1 [https://perma.cc/Z59P-URP5] (full list of member companies).

51 *About the NAI*, *supra* note 48; NETWORK ADVERT. INITIATIVE, 2020 NAI CODE OF CONDUCT 1 (2020) [hereinafter NAI CODE OF CONDUCT], https://www.networkadvertising.org/sites/default/files/nai_code2020.pdf [https://perma.cc/K2VE-SYWT].

52 NAI CODE OF CONDUCT, *supra* note 51, at 10–15.

53 *Id.* at 10.

54 *Id.*

55 *Id.* at 13.

56 *Id.* at 9.

57 *Id.* at 24.

accountable, and members are not always compliant with their own requirements.[58]

NAI member compliance with notice, education, and consent requirements often takes the form of detailed privacy policies.[59] The problem with these policies, however, is that they are often too dense for users to reasonably read them.[60] Additionally, even if users read privacy policies, studies show that the average lay internet user cannot sufficiently decode the complex, verbose descriptions of how their data gets stored and used.[61] As a result, the NAI Code of Conduct requirements may not adequately protect users. NAI members cannot truly obtain the consent they require from internet users to collect and store sensitive data if the users do not understand the scope of the consent they are giving. The sentiment behind requiring consent and the process of subsequently obtaining consent are thus mismatched.

The NAI enforces its requirements in a self-regulatory manner, meaning NAI member companies evaluate and adjust their own compliance via self-assessments and user complaints.[62] The NAI sometimes refers matters to the FTC for evaluation, but the NAI generally decides for itself how the Code of Conduct applies.[63] Moreover, even when matters are referred to the FTC and litigated, NAI members are not always held accountable for violations.

For example, in *United States v. Google*, Google paid a civil penalty for an alleged violation of an FTC order to comply with consent requirements, but there was one caveat—Google paid the penalty without admitting liability.[64] The FTC initially brought suit alleging that Google improperly used Gmail users' information and automatically enrolled them in its social networking platform, Google

---

58 *See generally* Saranga Komanduri et al., *Ad Choices? Compliance with Online Behavioral Advertising Notice and Choice Requirements*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 603 (2012) (presenting an NAI member compliance study that specifically analyzed members' notice and opt-out policies).

59 NETWORK ADVERT. INITIATIVE, GUIDANCE FOR NAI MEMBERS: OPT-IN CONSENT 6 (Nov. 2019), https://www.networkadvertising.org/sites/default/files/nai_optinconsent-guidance19.pdf [https://perma.cc/8N4U-CHS2].

60 Komanduri et al., *supra* note 58, at 607.

61 Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 83 (2015).

62 NAI CODE OF CONDUCT, *supra* note 51, at 16.

63 *Id.* at 6.

64 United States v. Google, Inc., No. CV 12-04177 SI, 2012 WL 5833994, at *2 (N.D. Cal. Nov. 16, 2012).

Buzz, despite statements that it would not.[65] Google settled the case by entering a consent order with the FTC, which prohibited Google from further misrepresenting its data collection practices.[66] The FTC later alleged, however, that Google violated the consent order by overriding Safari users' ability to opt out of Google's data collection and continuing to collect users' information.[67] In response, Google signed a stipulated judgment, agreeing to pay a large civil penalty and delete any cookies that improperly collected Safari users' information.[68] But despite paying a penalty and adjusting its systems, Google denied that it ever violated the FTC's order.[69] Thus, there is no record that Google's conduct constituted a violation, which suggests that the NAI Code of Conduct is not always strictly enforced—even when the most serious matters are referred to the FTC.

3. Federal Statutes

Although one might expect federal statutes to clarify how constitutionally enumerated rights like the right of privacy get protected, federal statutes have only fractured and segmented the scope of data privacy protections. Under current federal law, only specific types of data held by specific entities receive protections. Consequently, United States citizens' data can be subject to numerous procedures and standards, or none at all, depending on the context.

For example, the Health Insurance Portability and Accountability Act (HIPAA) generally protects patients' privacy rights in their medical information.[70] Notably, however, HIPAA protections depend on the type of information held and who holds it.[71] Thus, while information like a patient's HIV status may be protected when electronically stored by a healthcare provider, that same information is not subject to HIPAA protections if an individual provides it on a mobile app unrelated to health care.[72] Moreover, even if information

65 *Id.* at *1.

66 *Id.*

67 *Id.*

68 *Id.* at *2.

69 *Id.*

70 *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

71 *See* 45 C.F.R. § 160.103 (2020); 87 AM. JUR. 3D *Proof of Facts* § 5 (2006).

72 *See* 87 AM. JUR. 3D *Proof of Facts* § 5 (2006). A dating app, for example, would not fit HIPAA's definition of a covered entity, and thus the sharing of HIV status on a dating app would not be protected by HIPAA.

regarding HIV status is subject to HIPAA protections, HIPAA itself sets out situations in which the information becomes subject to state law,[73] adding another layer of complication to the already tangled method of protecting sensitive data.

Federal statutes protect other sector-specific types of data as well, such as educational records[74] and financial information.[75] Certain documentary materials and work products are also subject to protection from search and seizure,[76] but these protections have become unclear as technology has changed the way we share information.[77] The existence of these sector-specific statutes merely bandages certain types of privacy injuries and leaves many other privacy interests vulnerable to intrusion. These sector-specific statutes also make the method of protecting privacy overcomplicated and seem to beg for a more uniform system.

C. Identifying a Gap

Privacy is both intuitively and constitutionally recognized as important to United States residents.[78] But despite its importance, no uniform system has been developed to protect data privacy interests in the digital age. Rather, a complicated web of thin protections has been woven to solve problems as they have arisen. The problem with this web is that it is filled with gaps—gaps that leave internet users vulnerable to their information falling outside their control. Internet users in the United States have no uniform way of seeking a legal remedy for invasions of data privacy, even as they become more and more dependent on the internet. Thus, it is high time for Congress to standardize the way the United States treats the collection, storage, and transmission of its residents' data.

---

73 *Id.* § 18.

74 Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

75 Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x.

76 Privacy Protection Act of 1980 (PPA), Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended in scattered sections of 42 U.S.C.).

77 Elizabeth B. Uzelac, *Reviving the Privacy Protection Act of 1980*, 107 NW. U. L. REV. 1437, 1451–52 (2013).

78 *See supra* Section I.A.

II
OTHER DATA PRIVACY SCHEMES

A. The European Union's General Data Protection Regulation

In 2016, the European Union took a momentous step by introducing the General Data Protection Regulation (GDPR), which greatly expanded and uniformly outlined the privacy rights of European internet users.[79] The GDPR took effect in 2018 and set a minimum standard of data protection with which each member state must comply.[80] The European Union had previously attempted to regulate data privacy through the European Union Data Protection Directive, but the Directive only set forth principles for each member state to incorporate into its own unique privacy schemes.[81] Thus, the GDPR took what was once a patchwork system of data protection and, for the first time, set a uniform level of protection across the entire European Union.[82]

1. The GDPR's Features

The GDPR's text begins with the overarching principles and sentiments behind regulating data more carefully.[83] The GDPR notes that principles of "lawfulness, fairness and transparency" must guide the way personal data is processed,[84] and reasonable steps must be taken to maintain the data's accuracy.[85] Additionally, data collection must be limited to "specified, explicit[,] and legitimate purposes,"[86] and the data must be stored only for as long as is necessary to fulfill those purposes.[87] The quantity of stored data must also be minimized and limited to the amount necessary to fulfill the relevant purposes.[88] All the while, data must be processed in a way that guarantees

79 Peta-Anne Barrow et al., *International Privacy Law*, *in* PROSKAUER ON PRIVACY 14-1, 14-9 to -10 (Kristen J. Mathews ed., 2d ed. 2018).

80 *Id.* at 14-9.

81 *Id.*

82 *Id.* at 14-10.

83 Regulation 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), art. 5, 2016 O.J. (L 119) 35, 36 [hereinafter GDPR].

84 *Id.* art. 5(1)(a). "Personal data" is defined as "any information relating to an identified or identifiable natural person." *Id.* art. 4(1).

85 *Id.* art. 5(1)(d).

86 *Id.* art. 5(1)(b).

87 *Id.* art. 5(1)(e).

88 *Id.* art. 5(1)(c).

"integrity and confidentiality" for data subjects.[89] Finally, the GDPR sets forth a principle of "accountability," holding data controllers responsible for demonstrating their compliance on their own accord.[90]

The GDPR also provides an explicit set of rights for data subjects,[91] giving data subjects more control over their relationships with data controllers. For example, data subjects in the European Union now have the right to access a report from controllers detailing what data is being processed and how it is being processed.[92] Data subjects also have the right to correct inaccuracies in their data[93] and even completely erase pieces of their data in certain circumstances, including when their data has been processed unlawfully, their data is no longer necessary for fulfilling relevant purposes, or they have withdrawn requisite consent.[94] Data subjects may also object to their data being processed for the public interest or the interests of controllers, and controllers can overcome an objection only if they can demonstrate a "compelling[,] legitimate" reason to override the data subject's rights.[95]

Under the GDPR, data subjects may also refuse to be subject to automated processing decisions.[96] These processing decisions explicitly include those that produce legal effects or other significant effects based on profiling.[97] Additionally, data subjects in the European Union have the right to receive a portable, "commonly used and machine-readable" copy of their data from a controller so they can transmit the data to a different controller without hindrance.[98] Finally,

---

89 *Id.* art. 5(1)(f). Although the GDPR does not define "data subject," the term encompasses anyone whose data gets held, controlled, or processed. *What Is a Data Subject?*, EU GDPR COMPLIANT, https://eugdprcompliant.com/what-is-data-subject/ [https://perma.cc/G8U2-A34D].

90 GDPR, *supra* note 83, art. 5(2). A data "controller" is a "natural or legal person, public authority, agency[,] or other body which . . . determines the purposes and means of the processing of personal data." *Id.* art. 4(7).

91 *Id.* arts. 15–22. Specifically, the GDPR gives data subjects the right of access, the right to rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object to data processing, and the right to not be subject to automated decision-making. *Id.*; Barrow et al., *supra* note 79, at 28–30.

92 GDPR, *supra* note 83, art. 15.

93 *Id.* art. 16.

94 *Id.* art. 17.

95 *Id.* art. 21.

96 *Id.* art. 22(1).

97 *Id.*

98 *Id.* art. 20.

data subjects have the right to restrict the processing of their personal data when they do not wish to object to processing wholesale but nonetheless have concerns with the lawfulness or accuracy of the controller's practices.[99]

Some of the rights outlined in these GDPR provisions existed in various forms while European Union member states were implementing their own systems, and other rights were newly introduced with the GDPR.[100] Ultimately, these rights, combined with the overarching principles of compliance, create a more concrete relationship between data subjects and data controllers, and these rights more evenly balance the level of control each party can exercise.

Another significant feature of the GDPR is its heightened standard when data practices require consent from data subjects.[101] To consent to a data controller's privacy policy, a data subject must freely give a "specific, informed[,] and unambiguous indication" that they agree with the terms of the processing.[102] This indication must be in the form of a "statement" or "clear affirmative action."[103] Thus, something like a pre-checked box is insufficient to show consent.[104] Rather, data subjects must affirmatively check the box on their own.[105] In addition, the GDPR heightens the standard even more for categories of data deemed to be sensitive.[106] This category of sensitive data includes information that reveals racial origin, religious beliefs, and sexual orientation.[107] Before any data falling into this category is processed, the data controller must separately receive "explicit consent" from the subject,[108] which can be provided via email, a signed document, or some other form.[109] Under this standard, data controllers must do much more than provide a box at the end of a catchall policy, as many data subjects are accustomed to.

---

99 *See id.* art. 18.

100 Barrow et al., *supra* note 79, at 28.

101 *Id.* at 27.

102 GDPR, *supra* note 83, art. 4(11).

103 *Id.*

104 Barrow et al., *supra* note 79, at 27.

105 *Id.*

106 GDPR, *supra* note 83, art. 9(1).

107 *Id.*

108 *Id.* art. 9(2)(a).

109 Barrow et al., *supra* note 79, at 27.

2. Enforcement and Remedies in the European Union

The GDPR outlines specific enforcement provisions to give these significant rights and responsibilities teeth.[110] Specifically, the GDPR gives data subjects both the right to file complaints with supervisory authorities (an administrative remedy, subject to judicial review)[111] and the right to file complaints in an individual capacity against data controllers and processors in a judicial forum.[112] The GDPR also allows nonprofit organizations to bring claims on behalf of data subjects, even without an explicit mandate from data subjects.[113] Accordingly, independent nonprofit organizations are empowered to investigate and pursue claims against data controllers and processors in the public interest.[114]

If an individual pursues a claim and successfully shows that they have been damaged—whether materially or immaterially—by an infringement of the rights discussed above, then that person is entitled to compensation from the responsible controller or processor.[115] For actions brought to supervisory authorities under administrative procedures, a set of factors determines the amount a liable party can be fined.[116] The compensation amounts calculated with these factors are subject to damage caps, but these caps are still substantial.[117] For example, failure to obtain adequate consent to use sensitive data is subject to a cap of €20,000,000 (approximately $22,379,125) or "up to

---

110 *See* GDPR, *supra* note 83, arts. 77–84.

111 *Id.* arts. 77–78.

112 *Id.* art. 79. A "processor" is an entity that processes personal data on behalf of a data controller. *Id.* art. 4(8). Processors and controllers may be attributed differing levels of liability depending on their relationship and the extent of their fault. *See id.* art. 82(2)–(5).

113 *Id.* art. 80.

114 *See id.*

115 *Id.* art. 82.

116 *Id.* art. 83(2). Article 83 of the GDPR provides eleven factors for determining an appropriate fine: (1) the nature, gravity, and duration of the infringement; (2) the intent or negligence involved in the infringement; (3) the extent to which actions were taken to mitigate damage; (4) the degree or responsibility of controllers and processors based on their organizational setup; (5) relevant previous infringements; (6) the degree of cooperation to remedy the infringement and mitigate future effects; (7) the categories of data involved in the infringement; (8) the way the infringement became known, including whether the controller or processor came forward on their own; (9) whether the controller or processor has complied with previous orders concerning the same subject matter; (10) whether the controller or processor has adhered to approved codes of conduct or certification mechanisms; and (11) any factors that aggravate or mitigate the circumstances of the infringement. *Id.*

117 *Id.* art. 83(3)–(6).

4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."[118] Thus, even within the limits of damage caps, data controllers and processors may be liable for significant amounts depending on the nature of their noncompliance.

Also, for any actions brought outside the administrative procedures (i.e., actions brought straight to a judicial forum), the GDPR leaves authority in the hands of European Union member states to set penalty rules, so long as the penalties are "effective, proportionate[,] and dissuasive."[119] Under such an enforcement scheme, the European Union has consequently taken one of the largest steps toward achieving effective and uniform data privacy practices.

B. The California Consumer Privacy Act

More recently, California has also taken steps to protect its residents' data in the age of rapid technological development.[120] The state enacted the California Consumer Privacy Act (CCPA) in 2018, and the law officially took effect on January 1, 2020.[121] The law was later expanded and amended in November 2020 when California passed Proposition 24, also known as The California Privacy Rights Act of 2020.[122] The CCPA is said to be the most comprehensive piece of legislation to address privacy in the United States, although it does not quite reach the strict, sweeping influence of the GDPR.[123] Unlike the GDPR, which applies to all European Union data processors and controllers,[124] the CCPA applies only to large, for-profit businesses that meet certain threshold requirements involving annual gross revenues and data sales.[125] Nonetheless, the CCPA puts forth new and

---

118 *Id.* art. 83(5). The conversion from Euros to American dollars was calculated using the exchange rate as of March 15, 2020. *US Dollar Exchange Rates for March 15, 2020 Against Currencies in Europe*, EXCHANGE-RATES (Mar. 15, 2020), https://www.exchange-rates.org/HistoricalRates/E/USD/3-15-2020 [https://perma.cc/EV3U-295P].

119 GDPR, *supra* note 83, art. 84(1).

120 Kari Paul, *California's Groundbreaking Privacy Law Takes Effect in January. What Does It Do?*, THE GUARDIAN (Dec. 30, 2019, 3:00 PM), https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do [https://perma.cc/LPC8-NQV9].

121 *Id.*

122 California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24 (West) (to be codified at CAL. CIV. CODE § 1798). The amendments will take effect in 2023.

123 *Id.*

124 *See* GDPR, *supra* note 83, arts. 2–3.

125 Elaine F. Harwell, *What Businesses Need to Know About the California Consumer Privacy Act*, A.B.A. (Oct. 7, 2019), https://www.americanbar.org/groups/business_law/publications/blt/2019/10/ca-consumer-privacy/ [https://perma.cc/N8Y2-RM7G].

unique rights for California residents and provides the opportunity for relief if businesses infringe those rights.

1. The CCPA's Features

The CCPA explicitly notes that it was born out of the constitutionally protected right of privacy[126] and is thus intended to provide the greatest protection possible for California residents.[127] To ensure that the greatest protections are provided, the CCPA clarifies that its provisions apply to all personal information collected or sold by businesses, not just to electronic or internet information.[128] Additionally, if the CCPA comes into conflict with another law, the CCPA concedes that the law that more adequately protects the constitutional right of privacy should govern.[129]

Similar to the GDPR, the CCPA gives California "consumers" a set of unique rights in their data.[130] For instance, the CCPA gives Californians the right to access categories and specific pieces of their personal data being collected and sold by businesses.[131] Businesses must provide at least two methods for consumers to make these requests free of charge.[132] Furthermore, the CCPA gives consumers the right to delete data that businesses have collected.[133] This right is not limited to particular circumstances,[134] but it comes with a list of exceptions—including when maintaining a consumer's data is necessary to complete a transaction, provide a good or service

Specifically, the CCPA applies to entities that do business in California and meet one of the following thresholds: having annual gross revenues of more than $25 million; selling or sharing the information of at least 100,000 consumers, households, or devices; or deriving at least half of annual revenues from selling consumers' personal information. CAL. CIV. CODE § 1798.140(c)(1)(A)–(C) (West 2020).

126 CIV. § 1798.175 (West 2020).

127 *See id.*

128 *Id.*

129 *Id.*

130 DATAGUIDANCE & FUTURE OF PRIV. F., COMPARING PRIVACY LAWS: GDPR V. CCPA 25–37 (Dec. 2019), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf [https://perma.cc/MC98-7HVA]. The CCPA broadly defines a "consumer" as any natural person who is a California resident. CIV. § 1798.140(g) (West 2020).

131 CIV. § 1798.100(a) (West 2020).

132 *Id.* § 1798.130(a)(1)(A). If the business maintains a website, the business must make the *website* available as a method for submitting requests. *Id.* § 1798.130(a)(1)(B) (emphasis added).

133 *Id.* § 1798.105(a).

134 *See id.*

requested by the consumer, ensure the security and integrity of the data, engage in scientific research, or exercise free speech.[135]

The CCPA also provides consumers the right to opt out of their data being sold or shared.[136] Unlike the GDPR, which provides data subjects an ongoing right to object to data processing as issues arise,[137] the CCPA gives consumers the ability to remove themselves at the outset from situations in which their data would be sold.[138] To further this right for consumers, businesses must provide "clear and conspicuous link[s]" on their websites saying "Do Not Sell My Personal Information."[139] Businesses must also explain the right to opt out in their privacy policies.[140] Notably, businesses cannot combat consumers' requests to not have their data sold,[141] and "selling" is very broadly defined to include essentially any transaction, transfer, or release of data completed for "monetary or other valuable consideration."[142] California consumers thus have a very powerful tool to protect themselves wholesale from certain data practices.

2. Enforcement and Remedies in California

The rights and responsibilities under the CCPA are enforced by the California Attorney General through administrative processes.[143] The Attorney General is responsible for soliciting public participation to create regulations that update and clarify the provisions of the CCPA,[144] reflecting a usual notice-and-comment administrative procedure. And, due to the passage of Proposition 24, California will have a new state agency called the California Privacy Protection Agency involved in this process. For the most part, the California Privacy Protection Agency holds the power to assess violations and issue fines.[145] Individuals do, however, hold a more limited power to

---

135 *Id.* § 1798.105(d)(1)–(9).

136 *Id.* § 1798.120(a).

137 GDPR, *supra* note 83, art. 21.

138 CIV. § 1798.120(a).

139 *Id.* § 1798.135(a)(1).

140 *Id.* § 1798.135(a)(2)(A).

141 *See id.* § 1798.120. This differs from the GDPR, which allows data processors and controllers to override data subjects' objections with compelling, legitimate reasons for keeping data. GDPR, *supra* note 83, art. 21.

142 CIV. § 1798.140(t)(1).

143 *See id.* §§ 1798.155, 1798.185.

144 *Id.* § 1798.185.

145 California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24, § 17 (West) (to be codified at CAL. CIV. CODE § 1798.155).

bring civil actions on their own behalf when their "nonencrypted and nonredacted personal information" has been subject to "unauthorized access and exfiltration, theft, or disclosure" due to a business's failure to appropriately secure the information.[146] In other words, the agency may pursue claims for all CCPA violations, and individuals may pursue claims only for data breaches. This means individuals would not be able to pursue their own claims for a business's failure to provide the ability to opt-out of data sales, for example.

Businesses that violate the CCPA may face fines issued by the California Privacy Protection Agency. Fines are limited to $2,500 for each unintentional violation and $7,500 for each intentional violation,[147] although there is no limit on the total fine that may be issued if several violations are found.[148] The proceeds acquired from these fines then get deposited into the Consumer Privacy Fund,[149] a state fund created by the CCPA to offset the state courts' costs of adjudicating data privacy actions and the costs of the Attorney General's administrative duties.[150]

An individual pursuing a civil action for data breaches must provide a thirty-day window for businesses to cure alleged violations.[151] If the alleged violations are not cured within thirty days, the individual can then bring the action into court and seek damages—either damages within the range of $100 to $750 per violation, or actual damages, whichever is higher.[152] Consumers also have the ability to pursue class actions with the same process and damages available.[153] To determine the appropriate amount of damages to award, courts will apply any one or more of the factors listed in the CCPA.[154] Additionally, courts may award injunctive or declaratory relief to individuals or classes.[155] Although this system is still fairly limited due to the low damage caps

146 CIV. § 1798.150(a)(1).

147 *Id.* § 1798.155(b).

148 *See id.*

149 *Id.* § 1798.155(c).

150 *Id.* § 1798.160.

151 *Id.* § 1798.150(b).

152 *Id.* § 1798.150(a)(1)(A).

153 *Id.* § 1798.150(b).

154 *Id.* § 1798.150(a)(2). The non-exhaustive list of factors for determining appropriate damages is as follows: the nature and seriousness of the misconduct; the number of violations; the persistence of the misconduct; the time period over which misconduct occurred; the willfulness of the misconduct; and the defendant's assets, liabilities, and net worth. *Id.*

155 *Id.* § 1798.150(a)(1)(B).

and restrictions on the types of actions that can be brought, the opportunity to seek compensation for data privacy violations is novel for the United States and presents a practical remedy when viewed in tandem with the administrative enforcement.[156]

III
THE LGBTQ EXPERIENCE ONLINE

Because the current state of United States data privacy leaves particular communities vulnerable to information leaks, one might suggest that the most vulnerable communities should exercise greater caution online or reduce their internet presence. To be clear, this Comment rejects this suggestion as a solution. The breadth of information available online and the opportunities to communicate with like-minded individuals make the internet an extremely significant part of life for the LGBTQ community. Although it is true that certain incidents have illuminated the risks of LGBTQ participation in online communities, the solution should not be to abandon the significant opportunities that are available. Rather, those opportunities should be made safer through greater data privacy protections.

The growth and development of the digital environment has created a hub for LGBTQ youth.[157] The broad scope of information available online provides LGBTQ youth a place to explore the spectrum of sexual orientation and gender identity, develop a better sense of personal identity, and interact with like-minded people.[158] Having space to learn and engage in discussions about the LGBTQ experience is crucial for LGBTQ people to understand their own identities.[159] Lingering social norms and stigmatization surrounding LGBTQ people, however, still affect the way community members approach their identity exploration.[160] For many, this exploration needs to happen in secret, whether for fear of being disowned, outcasted, or

---

156 Recall that the GDPR sets much higher damage caps and allows individuals to bring actions for any violation of the GDPR, not just data breaches. *See* discussion *supra* Section II.A.2.

157 *See* Jesse Fox & Rachel Ralston, *Queer Identity Online: Informal Learning and Teaching Experiences of LGBTQ Individuals on Social Media*, 65 COMPUTS. HUM. BEHAV. 635, 636 (2016).

158 *Id.*

159 *See id.* at 640–41.

160 *See* Shelley L. Craig & Lauren McInroy, *You Can Form a Part of Yourself Online: The Influence of New Media on Identity Development and Coming Out for LGBTQ Youth*, 18 J. GAY & LESBIAN MENTAL HEALTH 95, 98 (2014).

physically hurt.[161] Consequently, there are two competing interests for the LGBTQ community online: the interest in exploring identity and the interest in remaining private.

Over the years, LGBTQ youth have figured out a few ways to balance these competing interests. Tumblr, for example, became a popular site for LGBTQ youth to post and view content in the 2010 decade.[162] Tumblr introduced a platform where users could create their own "blogs" and follow other blogs with content matching their interests.[163] The nature of this platform led most users to operate blogs separate from their usual social circles at school or within their local community (unlike sites like Facebook).[164] As a result, Tumblr users enjoyed a certain level of anonymity if they chose not to disclose their names or faces. This anonymity thus allowed LGBTQ youth to find and share content to develop an understanding of their sexual orientation or gender identity without compromising their interest in keeping their intimate details secret from the people in their daily lives.[165]

YouTube also arose as a popular platform for LGBTQ identity exploration.[166] As some YouTube users became comfortable with sharing their coming out stories on the video streaming site, large audiences of LGBTQ youth could consume these stories.[167] Having such content easily accessible allowed many LGBTQ youth to see how similar individuals overcame challenges and became happier with their identities.[168] All the while, the youth consuming these videos did not have to reveal their own identities, either offline or online.[169] Consequently, YouTube provided space for youth to explore their own identities and enjoy commonalities with other LGBTQ individuals while maintaining anonymity.[170]

Because the internet is such a significant space for members of the LGBTQ community, it is imperative that LGBTQ internet users are

---

161 *See id.* at 104 (noting that anonymity allows for safer identity exploration in the face of homophobia and transphobia offline).

162 *See* Fox & Ralston, *supra* note 157, at 639.

163 About Page, TUMBLR, https://www.tumblr.com/about [https://perma.cc/PWV9-NS9Z].

164 Fox & Ralston, *supra* note 157, at 639.

165 *See id.*

166 Craig & McInroy, *supra* note 160, at 102–03.

167 *Id.* at 102.

168 *Id.* at 103.

169 *Id.* at 102–03.

170 *Id.*

protected. Historically, however, the community has been vulnerable to data leaks and inappropriate use of information. For example, Grindr, a popular LGBTQ dating app, has a concerning history with the way it manages its users' data.[171] In 2018, Grindr faced backlash after a report revealed that the app had been sharing personal data with outside vendors.[172] The data being shared included users' HIV statuses, which represented a particularly egregious invasion of privacy for Grindr users who were HIV-positive.[173] Because HIV status was—and still is—highly stigmatized in the United States, this disclosure of positive statuses posed serious discrimination concerns for Grindr users.[174] Grindr contended that it always transmitted users' data with encryption and made efforts to limit sharing information, but the app ultimately changed its policy altogether and stopped sharing HIV status.[175] Unfortunately, however, this was only one incident out of multiple.

Within the same year, Grindr also faced criticism for a flaw in its data security system that had the potential to leak millions of users' personal information.[176] The flaw was exposed when a third party created a website where Grindr users could link their accounts and pinpoint which users had blocked them on the dating app.[177] When Grindr users began linking their accounts to this website, the site creator discovered he had access to users' deleted photos, unread messages, email addresses, and GPS locations—even for users who had opted not to share their location data publicly on the Grindr app.[178] In response, Grindr warned its users to not share their account information

---

171 *See* David Pierson, *Gay Dating App Grindr Changes Its Policy of Sharing Users' HIV Status with Outside Vendors*, L.A. TIMES (Apr. 2, 2018, 5:41 PM), https://www.latimes.com/business/technology/la-fi-tn-grindr-hiv-data-20180402-story.html; Brian Latimer, *Grindr Security Flaw Exposes Users' Location Data*, NBC NEWS, https://www.nbcnews.com/feature/nbc-out/security-flaws-gay-dating-app-grindr-expose-users-location-data-n858446 [https://perma.cc/USV2-M3R4] (Mar. 30, 2018, 9:34 AM); Janet Burns, *Report Says Grindr Exposed Millions of Users' Private Data, Messages, Locations*, FORBES (Mar. 29, 2018, 1:14 PM), https://www.forbes.com/sites/janetwburns/2018/03/29/report-says-grindr-exposed-millions-of-users-private-data-messages-locations/#33d1e1ba5c4c [https://perma.cc/4HA7-HSKK].

172 Pierson, *supra* note 171.

173 *Id.*

174 *Id.*

175 *Id.*

176 Burns, *supra* note 171.

177 *Id.*

178 *Id.*

with third parties.[179] The app also updated its data security system to disallow access to the blocked account data in order to discourage the third party from continuing to operate his website.[180] Notably, however, Grindr did not make any changes to disallow access to the other data.[181]

Grindr once again came under fire at the start of 2020 for sharing personal information such as age, gender, and sexual orientation with thousands of online advertisers.[182] Effectively, every time Grindr users opened the app, Grindr permitted advertising networks to gain private information about the users' internet behaviors and demographics to profile them for targeted advertisements.[183] This news became public following a Norwegian Consumer Council (NCC) report,[184] which analyzed the app's privacy policy.[185]

Specifically, the NCC noted that Grindr's privacy policy may have violated the European Union's GDPR due to accountability shifting and vagueness.[186] The NCC pointed to the fact that the Grindr privacy policy had to be accepted in its entirety upon downloading the app and that the app itself provided no additional information regarding the use of personal data.[187] By accepting this privacy policy at the outset, Grindr users consented to sharing information about their location, their profile, and some of their demographics with advertisers.[188]

But this term of the privacy policy also states that all the advertising partners' privacy policies apply to personal data obtained by Grindr,

---

179 Latimer, *supra* note 171.

180 *Id.*

181 *Id.* ("Two years after the location data was first revealed and addressed by Grindr, security researchers found they were still able to figure out users' locations.").

182 Suhauna Hussain et al., *Grindr, Tinder and OkCupid Apps Share Personal Data, Group Finds*, L.A. TIMES (Jan. 14, 2020, 5:20 PM), https://www.latimes.com/world-nation/story/2020-01-14/dating-apps-leak-personal-data-norwegian-group-says [https://perma.cc/FA3L-SZQT].

183 *Id.*

184 *Id.*

185 NORWEGIAN CONSUMER COUNCIL, OUT OF CONTROL: HOW CONSUMERS ARE EXPLOITED BY THE ONLINE ADVERTISING INDUSTRY 72–74 (2020), https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf [https://perma.cc/3ZYK-P7CN].

186 *Id.* at 74.

187 *Id.* at 72.

188 *How We May Share Data*, GRINDR, https://www.grindr.com/privacy-policy/how-we-may-share/?lang=en-US [https://perma.cc/EXK9-AN72] (Dec. 8, 2020).

while identifying only one of those advertising partners.[189] Consequently, Grindr users may be subject to the policies of numerous third-party advertising companies that the users have no way of finding.[190] The NCC report argued that this term violates the GDPR because it attempts to shift the control over personal data away from Grindr itself.[191] Additionally, NCC argued that this policy is overly vague and forces Grindr users to consent to a data collection system they can never fully understand.[192]

Although this NCC report pointed to potential violations under the European Union's privacy scheme, the report nonetheless sparked interest in the United States.[193] In particular, the report raised questions about whether Grindr's updated privacy policy failed to comply with California's newly enacted CCPA.[194] At the time of NCC's report, the CCPA required companies to provide an opportunity to opt out of the practice of selling personal data, but Grindr arguably does not do this.[195] Grindr does not offer specific opt-out opportunities; rather, Grindr asks users to consent to its entire privacy policy, which states that the app can "collect, use, share, and retain" but does not sell its users' personal data.[196] Furthermore, consent from users allows Grindr to disclose particular categories of information to third-party advertisers.[197] Thus, Grindr's attempts at writing around the opt-out requirement may violate California residents' newly bestowed privacy rights. Without these privacy rights, Grindr's policy would proceed unchecked, leaving its LGBTQ users vulnerable and without recourse.

---

189 *Id.* ("The privacy policies of the third-party companies apply to their collection, use and disclosure of your Personal Data. One of our main advertising partners is MoPub that helps Grindr deliver personalized advertising.").

190 NORWEGIAN CONSUMER COUNCIL, *supra* note 185, at 74.

191 *Id.*

192 *Id.*

193 Hussain et al., *supra* note 182.

194 *Id.*

195 *Id.* With the passing of Proposition 24 in California, the CCPA will also require that companies provide an opportunity to opt out of "sharing" personal data. California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Proposition 24, § 9 (West) (to be codified at CAL. CIV. CODE § 1798.120).

196 *Grindr Privacy and Cookie Policy*, GRINDR, https://www.grindr.com/privacy-policy/?lang=en-US [https://perma.cc/SLA3-F2ZM] (Dec. 8, 2020).

197 *How We May Share Data*, *supra* note 188.

IV
PROPOSING A SOLUTION

As this Comment has demonstrated, the United States lacks a uniform method of protecting data privacy; instead, the United States has a patchwork system of protections, full of gaps that leave communities like the LGBTQ population vulnerable to data leaks and inappropriate data uses.[198] Because this gap-filled effort at protecting data privacy is insufficient, it is time for the United States to move forward the way the European Union and California have. Thus, this Part calls for data privacy legislation at the federal level and proposes a framework for such legislation to follow. The proposed framework takes inspiration from the GDPR and CCPA and tailors their provisions to develop the appropriate scope, responsibilities, rights, and enforcement strategies for the United States. This Part also addresses concerns regarding the potential for intellectual property infringement and the feasibility of implementing a new system.

A. The United States Framework

To create a uniform system that subsequently protects vulnerable communities, a United States data privacy scheme would need to be broadly applicable. Therefore, the scope of potential federal data privacy legislation should be analogous to that of the GDPR: the responsibility to comply should fall on all data controllers and processors who handle the data of United States residents.[199] California's model that imposes CCPA responsibilities only on large businesses that meet threshold profit and data transaction requirements[200] would not sufficiently further the goal of uniformity. The California model may protect its residents from large technology companies infringing on their privacy, but it inherently leaves gaps in the protection by imposing different standards on different entities. The California model also leaves the door open for companies to design their business models around the threshold requirements and thus avoid strict responsibilities. Consequently, for the sake of uniformity and effective protection, the United States is better off creating a system that applies to all collection, storage, and use of United States residents' data.

---

198 *See* discussion *supra* Sections I.B.–C.

199 *See supra* Section II.A.

200 *See supra* Section II.B.

The United States should also follow the European Union's example regarding what responsibilities to impose on data controllers and processors. Just as the GDPR requires, a United States data privacy scheme should limit data collection to specific, legitimate purposes and limit data storage to the amount of time necessary to fulfill such purposes. Frontloading responsibilities on data controllers and processors in this way makes the goals of data privacy legislation clear and mitigates the potential for harm before harm ever occurs. Additionally, the United States should hold data controllers and processors accountable in the same manner as the European Union and require such entities to demonstrate their compliance. Not only would this accountability system be an effective check on data controllers and processors but it would also reveal areas in which data privacy protections were still lacking. As a result, a system that holds data controllers and processors responsible for limiting their practices and evaluating their own compliance would be the most effective model for the United States.

The United States should also take inspiration from both the GDPR and CCPA regarding residents' rights. More specifically, the United States should grant its residents the following: the right to access reports of how data is being collected, stored, and used; the right to correct errors in data; the right to object to data uses outside the data subject's interests; the right to erase data under particular circumstances; and the right to opt out of data sales. This set of rights should not perfectly mirror either the GDPR or CCPA; rather, it should incorporate the pieces of each that are most appropriate for a federal data privacy scheme, balancing data controllers' practicality concerns and data subjects' autonomy concerns.

For example, the rights to object to certain data uses and erase data under particular circumstances should more closely resemble the GDPR's model. The CCPA does not provide an ongoing right to object.[201] This right is important to include in a federal system, however, because it gives residents greater control over the accuracy of their data and a more active role in how their data is being used. Without the ongoing right to object, residents would lack a continuing line of communication with data controllers and would have only administrative and judicial forums for their complaints.

The right to erase data should also resemble the right as enumerated in the GDPR, which provides specific situations where erasing data is

---

201 *See* discussion *supra* Section II.B.1.

necessary.[202] The CCPA does not require particular circumstances for California's residents to exercise the right to erase their data; rather, the CCPA provides a long list of exceptions that businesses can invoke to avoid requests to erase data.[203] This ability to freely erase data unless a business can find an exception may be counterproductive, and it implicates issues with hackers and intellectual property infringers discussed later in Section IV.B. Thus, a United States federal data privacy scheme should enumerate specific circumstances for data erasure, similar to the GDPR.

Regarding the right of access and the right to opt out of data sales, however, the CCPA serves as a more appropriate example. The CCPA explicitly outlines a protocol for requesting data reports: businesses must have free-of-charge methods for requesting data, via phone, email, or website interface.[204] Explicitly requiring such a protocol makes the process of requesting data more accessible and user-friendly for residents who may be confused by the technical nature of data processing or unaware of their right to make requests. Accordingly, the United States should follow California's lead with respect to the right of access and require clear procedures for making data requests. Additionally, the United States should maintain the CCPA's right to opt out of data being sold,[205] which is not available under the GDPR. This right is significant, as a common concern with data privacy is that the data provided to one entity gets transacted out into the ether.[206] Maintaining a right to opt out enables residents to know exactly who has their data and prevent it from ending up in someone else's hands.

A federal data privacy scheme should also separately categorize sensitive data and require heightened levels of consent for processing this kind of data. Separately categorizing sensitive data in this way would be the most direct method of preventing the potential discrimination that this Comment has grounded itself in. Explicitly

---

202 As previously mentioned, the specific situations in which a data subject may request data erasure include when data has been processed unlawfully, data is no longer necessary for fulfilling relevant purposes, or the requisite consent has been withdrawn. GDPR, *supra* note 83, art. 7.

203 CAL. CIV. CODE § 1798.105(d)(1)–(9) (West 2020).

204 *Id.* § 1798.130(a)(1).

205 *Id.* § 1798.120.

206 *See* Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/9P4B-GKYC].

requiring clear, affirmative consent to use sensitive information, like LGBTQ status, would allow LGBTQ individuals to pursue their interests in identity exploration, knowing that a system is in place to protect the precise information they wish to keep private. Accordingly, heightened consent for sensitive data does the heavy lifting to balance the LGBTQ community's competing interests in uninhibited exploration and privacy.

In order to enforce the proposed framework, the United States should also follow California's example by designating supervisory authority to an administrative agency. While CCPA violations are assessed and pursued in court by the California Attorney General and the California Privacy Protection Agency, the United States could delegate authority to the FTC. The FTC already pursues data privacy actions under its current statutory mandate,[207] and the agency has expressed significant interest in taking on a larger role.[208] Consequently, the FTC is likely equipped to take on the role of overseeing data privacy under a more robust statutory scheme, especially considering how much clearer the FTC's role would be when given more specific procedures.

The United States should also follow the CCPA's model regarding individuals' ability to file actions in court.[209] For example, requiring a thirty-day window of notice to allow data controllers to correct mistakes would be an efficient and practical way for the United States to handle violations. Such a model, again, reinforces the communication between data subjects and data controllers while preventing data subjects from clogging courts with privacy actions. This model would also lead to much faster corrections than if courts adjudicated every potential claim. Because the harm and collateral effects of improperly used data are more significant than the monetary value that could be assigned, a system in which data subjects and data controllers quickly work together to cure the improper use furthers the purposes of data privacy protections better than abundant opportunities for monetary damages would.

B. Lingering Concerns

Some may argue that the United States should not create its own federal data privacy scheme because it may strain the enforcement of

---

207 *See* discussion *supra* Section I.B.1.

208 *See* FTC STAFF REPORT, *supra* note 39, at i–iv.

209 *See* discussion *supra* Section II.B.2.

intellectual property rights.[210] More specifically, assigning more expansive rights to internet users—such as the rights to erase data and object to disclosures—may make it more difficult for owners of exclusive intellectual property rights to identify infringers online.[211] For example, if a writer authored and shared an article on a personal blog and later found that another writer had appropriated a large portion of the article—infringing the original writer's copyright—the original writer would likely want to pursue the infringer.

Traditionally, the original writer would be able to do this by searching a directory of domain name registrants maintained by the Internet Corporation for Assigned Names and Numbers.[212] Through this directory, the original writer would be able to identify the infringer based on the domain name with which the infringer was associated, thus enabling the writer to pursue enforcement of their exclusive rights. If the infringer's rights in this scenario restricted the extent to which the controller of the directory data could disclose the infringer's identity, the original writer may run into a significant roadblock.

Fortunately for the writer in this scenario, however, the framework this Comment has proposed for a United States data privacy scheme leaves room to acquire the necessary identification information.[213] Under the proposed framework, data controllers and processors would be responsible for limiting their data practices to legitimate purposes; pursuing infringers of intellectual property should be considered a legitimate purpose. Therefore, data controllers and processors would have an avenue to justify disclosing the identities of infringers to owners of exclusive intellectual property rights without fear of violating the infringers' privacy rights.

Furthermore, a more uniform system of data privacy protection does not conflict with the United States intellectual property regime as much as this hypothetical scenario may suggest. In fact, a uniform data privacy system dovetails nicely with the purposes of copyright and

---

210 *See generally* Tara M. Aaron, *Availability of WHOIS Information After the GDPR—Is It Time to Panic?*, 108 TRADEMARK REP. 1129 (2018) (arguing that the GDPR makes it more difficult for brand owners to find the identities of trademark infringers); Patrick Wheeler & Mette Marie Kennedy, *Practical Tips on GDPR for Intellectual Property Attorneys*, A.B.A. (Feb. 1, 2019), https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2018-19/january-february/practical-tips-gdpr-intellectual-property-attorneys/ [https://perma.cc/ATX9-E2FV].

211 *See* Wheeler & Kennedy, *supra* note 210.

212 *See* Aaron, *supra* note 210, at 1132.

213 *See supra* Section IV.A.

patent protections. The Intellectual Property Clause of the United States Constitution gives Congress the authority to regulate the copyright and patent systems for the sake of "promot[ing] the [p]rogress of [s]cience and useful [a]rts."[214] The underlying purpose of having copyrights and patents is thus to encourage inventors, authors, and creators to give society new, innovative works; protecting data privacy helps further this purpose. With greater data protections, the internet would be a safer forum for all internet users, which would encourage a greater number of content creators to contribute to the progress the Constitution aims to promote.

One might also argue that the United States is simply not prepared to upend its current data practices and that enacting data privacy legislation would be burdensome for companies handling large amounts of consumer data. This argument fails, however, when considering the timeline of global data privacy progress. The United States would not be starting from scratch. The European Union's system, due to its broad scope, has already sparked large international companies to change their practices and come into compliance with a more stringent scheme.[215] Additionally, California's efforts have added another layer of compliance for companies maintaining data, and other states have also made strides toward protecting their residents' privacy online.[216]

With this information in mind, the question should not be whether companies are equipped to adjust to new privacy protections—companies have already had to adjust. Rather, the question should be whether companies are better equipped to tailor their practices to numerous privacy schemes or just one uniform scheme. If the concern is the burden of compliance, it logically follows that a singular scheme lessens the burden. Of course, a federal data privacy scheme would inevitably remain separate from something like the GDPR, so global companies would not be able to escape considering more than one set of responsibilities. But within the United States, Congress has the power to centralize the way data privacy is handled and move the

---

214 U.S. CONST. art. I, § 8, cl. 8.

215 *See* Rob Sobers, *The Average Reading Level of a Privacy Policy*, VARONIS, https://www.varonis.com/blog/gdpr-privacy-policy/ [https://perma.cc/V26Q-4NYT] (Mar. 29, 2020).

216 Carsten Rhod Gregersen, *The US Is Leaving Data Privacy to the States—and That's a Problem*, BRINK (Aug. 19, 2019), https://www.brinknews.com/the-us-is-leaving-data-privacy-to-the-states-and-thats-a-problem/ [https://perma.cc/WCU3-J94U] (noting that New York, Maine, Nevada, Maryland, Texas, and North Dakota have all taken steps to protect data privacy to varying extents).

country away from multiple state systems that impose different standards. Congress has the opportunity to ease the burden on companies holding large amounts of data while providing United States residents with crucial protections.

CONCLUSION

The rapid development of technology has created a world in which our personal data is ubiquitous. People around the globe carry cell phones, laptops, smart watches, and a number of other devices with them everywhere they go—and those devices have the power to string together each person's precise story using the abundance of information they hold. For some communities, the risk of this information being abused or leaked poses significant consequences. As this Comment has shown, the LGBTQ community in particular faces risks from the phenomenon of "outing" and potential discrimination at the hands of unprotected data. Thus, from the student who is afraid of being outed by advertisements on a public bus to the thousands of LGBTQ citizens who have had their HIV status leaked, the LGBTQ community presents a strong case for increased data privacy protections. While steps have been taken to afford greater protections in the European Union and California, the United States has yet to take steps at the federal level. This Comment, through the lens of the LGBTQ experience online, demonstrates why it is time for the United States to take those steps. To catch up with the global developments in data and to protect United States residents from harm, Congress must standardize this country's data privacy regime.