Volume 12 | Issue 1 Article 7

3-14-2022

THE FUTURE OF U.S. DATA PRIVACY: LESSONS FROM THE GDPR AND STATE LEGISLATION

Vanessa Perumal

THE FUTURE OF U.S. DATA PRIVACY: LESSONS FROM THE GDPR AND STATE LEGISLATION

Cover Page Footnote

Candidate for Juris Doctor, Notre Dame Law School, 2022; Master of Arts in International Relations, University of Chicago, 2015; Bachelor of Arts in Political Science, International Relations, and English Literature, University of Miami, 2014. I would like to thank my family for their love and support, especially my husband for inspiring me. Thank you to my colleagues on the Notre Dame Journal of International and Comparative Law for their thoughtful edits.

THE FUTURE OF U.S. DATA PRIVACY: LESSONS FROM THE GDPR AND STATE LEGISLATION

VANESSA PERUMAL*

INTRODUCTION

"…work on privacy and security is never done."—Sundar Pichai, Google CEO[1]

* Candidate for Juris Doctor, Notre Dame Law School, 2022; Master of Arts in International Relations, University of Chicago, 2015; Bachelor of Arts in Political Science, International Relations, and English Literature, University of Miami, 2014. I would like to thank my family for their love and support, especially my husband for inspiring me. Thank you to my colleagues on the Notre Dame Journal of International and Comparative Law for their thoughtful edits.

[1] Aditi Roy, *Google CEO says 'work on privacy and security is never done' as company adds privacy features to key products*, CNBC (May 7, 2019), https://www.cnbc.com/2019/05/07/google-ceo-says-work-on-privacy-and-security-is-never-done.html.

Over the past few years, governments have had to consider how to regulate personal information[2] within their jurisdictional reach. Such regulation was deemed necessary due to the onset of high-profile data breaches, invasions into computer networks, and other privacy concerns regarding third-party protection of personal information.[3] TikTok's sharing of eighty-nine million users' data to third-parties without consent and Google's failure to inform the public regarding a breach that jeopardized over five-hundred thousand users' information are just some of the many issues surrounding data privacy and regulation.[4] In response to these events and other data protection concerns, the European Union ("EU") and states such as California and Virginia have enacted privacy laws that give consumers improved control and access to their personal data.[5] Europe's General Data Protection Regulation ("GDPR")[6] set precedence as the world's first comprehensive data privacy legislation. Passed in 2018, the GDPR "gives all EU citizens easier access to their data, a right to portability, a right to be forgotten, and a right to learn when their data has been hacked."[7] Comparatively, the United States does not have a comprehensive law at the federal level and instead has a "patchwork of laws" enacted by the states.[8] Shortly after the GDPR took effect, California passed the California Consumer Privacy Act ("CCPA"),[9] one of the first U.S. laws to provide comprehensive consumer protection regulation for California residents. Additionally, several other states such as Maine and Illinois have also passed or are in the process of passing their own data privacy laws.[10]

---

[2] This Note uses the term "personal information" synonymously with "data protection," "personal data," and "data privacy." Personal information refers to identifying information such as name, date of birth, gender identity, sexual orientation, email address, and phone number. *See generally Data Protection*, EUROPEAN DATA PROTECTION SUPERVISOR, https://edps.europa.eu/data-protection/data-protection_en.

[3] *See generally* STEPHEN P. MULLIGAN, CONG. RESEARCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW (2019), https://fas.org/sgp/crs/misc/R45631.pdf.

[4] *See, e.g.*, Bobby Allyn, *TikTok To Pay $92 Million To Settle Class-Action Suit Over 'Theft' Of Personal Data*, NPR (Feb. 25, 2021, 6:11 PM), https://www.npr.org/2021/02/25/971460327/tiktok-to-pay-92-million-to-settle-class-action-suit-over-theft-of-personal-data; Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES, (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html; Allison Grande, *Google Data Leak Exposes Breach Disclosure Conundrums*, LAW360 (Oct. 12, 2018, 9:47 PM), https://www.law360.com/articles/1091877/google-data-leak-exposes-breach-disclosure-conundrums ("Google is facing widespread backlash after the revelation of its decision not to notify the public of an incident that exposed 500,000 users' data").

[5] *See generally* Alan Charles Raul, *Global Overview in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 416 (Alan Charles Raul ed., 6th ed. 2019), https://www.sidley.com/-/media/publications/united-states-2019.pdf?la=en.

[6] *See* Commission Regulation 2016/679, 2016 O.J. (L 119) (EU) [hereinafter GDPR].

[7] Michael L. Rustad, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365 (2019).

[8] MULLIGAN, *supra* note 3, at 2. Even with the Obama Administration's "Consumer Privacy Bill of Rights" in 2012, the effort to increase American control over their data at the federal level has been largely unsuccessful in the United States. *See generally* Natasha Singer, *Why a Push for Online Privacy is Bogged Down in Washington*, N.Y. TIMES (Feb. 28, 2016), https://www.nytimes.com/2016/02/29/technology/obamas-effort-on-consumer-privacy-falls-short-critics-say.html.

[9] 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West) (codified in CAL. CIV. CODE § 1798.100—1798.198).

[10] *See, e.g.*, Act to Protect the Privacy of Online Customer Information, S. P. 275 (Me. 2019), http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129. *See generally* Gretchen Ramos and Darren Abernathy, *Additional U.S. States Advance the State Privacy Legislation Trend in 2020*, NAT'L L. REV. (Dec. 15, 2020), https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020.

In addition to U.S. states enacting consumer privacy legislation, there has been pressure from both the private and public sector on Congress to create a federal data privacy legislation similar to the GDPR.[11] Technology giants from the private sector, such as Apple's CEO Tim Cook, stated to EU Officials that "[i]t is time for the rest of the world—including my home country—to follow your lead."[12] Google's CEO Sundar Pichai similarly wrote in an op-ed for *The New York Times* that he and others at Google "think the United States would benefit from adopting its own comprehensive privacy legislation and have urged Congress to pass a federal law."[13] Government agencies such as the U.S. Chamber of Commerce and Government Accountability Office have also recommended Congress pass such a law.[14] While there have been multiple attempts by both Democrats and Republicans to pass an overarching federal law, the United States remains without one.[15]

This Note supports the popular argument that there needs to be a federal data privacy law for two reasons: (i) the industry would benefit from a uniform standard that would provide a more streamlined approach to data privacy; and (ii) a comprehensive data privacy legislation will provide consumers uniform rights over their personal information. While the industry and current literature have supported a federal data privacy law, very few have analyzed the GDPR and U.S. state laws as sources to inform prospective legislation. Therefore, this Note compares current data privacy laws such as the GDPR and various proposed and enacted state laws from California, Virginia, Washington, and New York with the goal of identifying the parameters Congress can consider for the future legislative developments.[16] Based on a review of these laws, this Note also provides a normative discussion on the various features this type of legislation can include, such as uniform consumer rights, federal and state partnerships for enforcement, and the inclusion of a private right of action.

In Part I, this Note discusses the background and history of data privacy laws, with a focus on the EU and United States. Part II analyzes the GDPR as well as U.S. state consumer privacy legislation. Part III argues why there needs

---

[11] *See generally* Daniel J. Solove, *ALI Data Privacy: Overview and Black Letter Text*, 68 UCLA L. REV. 1 (2020).

[12] *See* Jonny Evans, *Complete Transcript, Video of Apple CEO Tim Cook's EU Privacy Speech,* COMPUTERWORLD (Oct. 24, 2018, 3:27 AM) https://www.computerworld.com/article/3315623/complete-transcript-video-of-apple-ceo-tim-cooks-eu-privacy-speech.html.

[13] *See* Sundar Pichai, *Google's Sundar Pichai: Privacy Should Not Be a Luxury Good*, N.Y. TIMES (May 7, 2019), https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html. Google has gone so far as to take matters into its own hands by promising to stop selling ads based on individual browsing data. *See* Sam Schechner & Keach Hagey, *Google to Stop Selling Ads Based on Your Specific Web Browsing*, THE WALL STREET JOURNAL (March 3, 2021, 6:15PM), https://www.wsj.com/articles/google-to-stop-selling-ads-based-on-your-specific-web-browsing-11614780021.

[14] Press Release, U.S. Chamber of Com., U.S. Chamber Releases Model Privacy Legislation, Urges Congress to Pass a Federal Privacy Law (Feb. 13, 2019), https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law; U.S. GOV'T. ACCOUNTABILITY OFF., CONSUMER PRIVACY: CHANGES TO LEGAL FRAMEWORK NEEDED TO ADDRESS GAPS (2019), https://www.gao.gov/products/GAO-19-621T (highlighting the need for an overarching federal privacy law).

[15] *See generally* GIBSON, DUNN & CRUTCHER, U.S. CYBERSECURITY AND DATA PRIVACY OUTLOOK AND REVIEW – 2021 (2021), https://www.gibsondunn.com/wp-content/uploads/2021/01/us-cybersecurity-and-data-privacy-outlook-and-review-2021.pdf.

[16] These states were selected because they have either proposed or already enacted data privacy legislation similar to the GDPR and CCPA as of February 2021.

to be a federal data privacy law and highlights the common factors Congress can consider for future legislation. Part IV concludes with a summary and next steps.

I. BACKGROUND

A. *DEFINING DATA PRIVACY AND DATA SECURITY*

This Note is interested in exploring both data privacy and data security as it pertains to personal information. Data privacy pertains to the manner in which companies and third-parties use and share non-public personal information, including but not limited to one's birthdate, name, gender identity, email, and telephone number.17 This non-public personal information is typically obtained from web browsing, warranty registrations, and retail loyalty cards, for example, compared to public information obtained from directories or newspapers.18 Relatedly, data security focuses on how companies "(1) protect personal information from unauthorized access or use and (2) respond to such unauthorized access of use."[19] Current U.S. legislation is preoccupied with both data privacy and data security as defined above.[20]

While many privacy laws share similarities with the United States' legislative interpretation of data privacy (especially Western liberal democracies such as the EU member states), other countries that have enacted data privacy laws take slightly different approaches based on their own specific issues.[21] As of February 2020, approximately 128 out of 194 countries have established some form of data privacy legislation (see Figure 2).[22] Non-western countries with relatively intrusive regimes—such as China—have no single definition of personal data.[23] But even China has attempted to enact a comprehensive law, and the draft (the Personal Information Protection Law as of October 2020) in its current form has been interpreted to mimic the GDPR.[24] The International Association of Privacy Professionals ("IAPP") explains that this draft law also reflects data protection principles including "transparency, fairness, purpose limitation, data minimization, limited retention, data accuracy and

---

[17] *See* EUROPEAN DATA PROTECTION SUPERVISOR, *supra* note 2. *See also* STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RESEARCH SERV. IF11207, DATA PROTECTION AND PRIVACY LAW: AN INTRODUCTION, 1 (2019), https://crsreports.congress.gov/product/pdf/IF/IF11207.

[18] U.S. GOV'T. ACCOUNTABILITY OFF., *supra* note 14, at 2.

[19] MULLIGAN & LINEBAUGH, *supra* note 17, at 1.

[20] *Id*.

[21] *See Data Protection Laws of the World*, DLA PIPER (2020), https://www.dlapiperdataprotection.com/index.html?t=about&c=BR.

[22] *Data Protection and Privacy Legislation Worldwide*, UNCTAD, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide [hereinafter UNCTAD] (highlighting sixty-six percent of countries have legislation, while thirty-four percent have draft or no legislation (or data).

[23] DLA PIPER, *supra* note 21, at 158.

[24] *See generally* HUNTON ANDREWS KURTH, *China Issues Draft Data Security Law*, PRIVACY & INFORMATION SECURITY LAW BLOG (2020), https://www.huntonprivacyblog.com/2020/07/07/china-issues-draft-data-security-law/; Amber L. Lawyer, Jessica L. Copeland, and Shannon A. Knapp, *The Great Wall of Data Privacy: China Passes Comprehensive Data Privacy Law*, BOND, SCHOENECK & KING (Aug. 31, 2021), https://www.bsk.com/news-events-videos/the-great-wall-of-data-privacy-china-passes-comprehensive-data-privacy-law.

accountability."[25] This step by China is not without its critics, however, and some have argued that China has gone too far in its surveillance efforts of its own citizens.[26] For example, recent litigation against WeChat, a Chinese multi-purpose messaging service, has presented a direct legal challenge to China's use of surveillance by this private company against its users.[27]

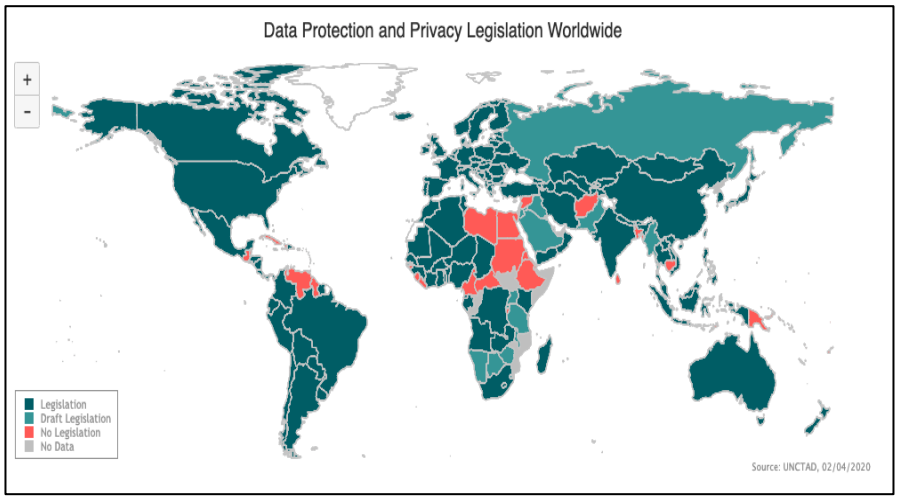

Figure 1. Data Protection and Privacy Legislation Worldwide (source: UNCTAD)[28]

B. *HISTORICAL APPROACHES TO DATA PRIVACY*

The EU and the United States share a common history as it pertains to the development of data privacy and security legislation.[29] As early as the 1980s, both countries participated in establishing the first set of internationally agreed-upon privacy principles as part of the Organisation for Economic Co-Operation and Development ("OECD") Guidelines Governing the Protection of Privacy and Transborder Flows of Data.[30] These Guidelines recognized the importance of personal information as well the possible impact on the rights of individuals

[25] Gil Zhang and Kate Yin, *A Look at China's Draft of Personal Information Protection Law*, INT'L ASS'N OF PRIVACY PROF'L (Oct. 26, 2020), https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.
[26] *See* Anna Mitchell & Larry Diamond, *China's Surveillance State Should Scare Everyone*, THE ATLANTIC (Feb. 2, 2018), https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/; Hashem Ahelbarra, *Is China Taking Social Monitoring too Far?*, ALJAZEERA (Feb. 19, 2019), https://www.aljazeera.com/program/inside-story/2019/2/19/is-china-taking-social-monitoring-too-far.
[27] *See* Jeanne Whalen, *California plaintiffs sue Chinese tech giant Tencent, alleging WeChat app is censoring and surveilling them*, THE WASH. POST (Jan. 20, 2021, 3:43PM), https://www.washingtonpost.com/technology/2021/01/20/wechat-class-action-lawsuit-us/ (discussing the company's practices violate the plaintiffs' free-speech and privacy rights and "unjustly enrich Tencent at the expense of California WeChat users").
[28] UNCTAD, *supra* note 22.
[29] *See generally* Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN. ST. J.L. & INT'L AFF. 49, n.56 (2020).
[30] *See* OECD, THIRTY YEARS AFTER THE OECD PRIVACY GUIDELINES, 1, 3 (2011), http://www.oecd.org/sti/ieconomy/49710223.pdf.

made possible by computer technology.[31] These Guidelines also provide core principles that are still embodied in privacy laws today, such as a protecting individual liberties, and "[ensuring] that the spread of privacy laws should not unduly restrict transborder data flows and the economic and social benefits they bring."[32] The OECD has updated these principles based on various changes in technology and data privacy since its inception over forty years ago, and both the United States and EU Member States remain parties.[33]

Despite sharing a common starting point, both the U.S. and EU differ in how they view data privacy, as well as how they have developed related legislation. Whereas the EU recognizes data privacy as a fundamental right, the United States—partly due to its sectoral approach—has developed varying interpretations of what constitutes data privacy and the protection of personal information. As one scholar puts it, "data protection is seen as a specific expression of the right to privacy" in the EU, whereas privacy in the United States is "currently a kind of 'hodgepodge' because it is not underpinned by a clear, unified right to privacy."[34] This section provides a brief overview of these diverging approaches to provide context for how each country came to develop their current data privacy legislation to date.

1. *The European Union's Right to Privacy*

The EU's view of data privacy as a fundamental right is deeply embedded in its jurisprudence, specifically at the constitutional level.[35] The two systems reflecting this right—the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union—will be discussed briefly. First, the European Convention on Human Rights,[36] which consists of all forty-seven Council of Europe member states, is an international treaty that seeks to protect human rights and fundamental freedoms.[37] Article 8 reflects the specific right to privacy, which states: "Everyone has the right to respect for his private and family life, his home and his correspondence."[38] Second, the Charter of Fundamental Rights of the European Union[39] takes these rights a step further by guaranteeing the right to the protection of personal information. This Charter bears the same legal value as the constitutional treaties of the EU, making the

---

[31] *Id*. at 3.
[32] *Id*. at 14.
[33] *Id*. at 3.
[34] Erdem Büyüksagis, *Towards a Transatlantic Concept of Data Privacy*, 30 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 139, 164–65 (2019).
[35] *EU Data Protection Directive*, ELEC. PRIVACY INFO. CTR. (2021), https://epic.org/privacy/intl/eu_data_protection_directive.html.
[36] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter European Convention on Human Rights] (entered into force Sept. 3, 1953).
[37] COUNCIL OF EUROPE, EUROPEAN UNION ACCESSION TO THE EUROPEAN CONVENTION ON HUMAN RIGHTS - QUESTIONS AND ANSWERS, (2020), https://www.coe.int/en/web/portal/eu-accession-echr-questions-and-answers. The EU is not itself a member.
[38] European Convention on Human Rights, *supra* note 36, at Article 8.
[39] Charter of Fundamental Rights of the European Union, 2000 O.J.(C364), 18 Dec. 2000. https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

EU institutions and bodies and the Member States bound by it.[40] Article 8 expressly identifies the right of the owner of the data:

> Everyone has the right to the protection of personal data concerning him or her . . . such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law . . . Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified . . . Compliance with these rules shall be subject to control by an independent authority.[41]

As this quote shows, the right to protection of personal data includes the right to access the data, as well as the right to have it rectified. These same rights are reflected in the GDPR and will be discussed further in Part II.

The rights described above have been addressed in over twenty-five years of Europe's data privacy legislation, well before the GDPR. Starting from 1995 during the internet boom, the EU passed the Data Protection Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data on the Free Movement of Such Data.[42] This Directive establishes a number of key legal principles ranging from fair and lawful processing of data to minimized data storage terms.[43] Twenty-eight of the EU Member states have applied these principles to their own national data protection laws.[44] This Directive "met to some extent its twin objectives of safeguarding the personal data of individuals and improving the flow of personal data among EU Member States."[45] However, after numerous data breaches and surveillance disclosures in the decades that

[40] *See* EUROPEAN DATA PROTECTION SUPERVISOR, DATA PROTECTION (last visited Sep. 21, 2021), https://edps.europa.eu/data-protection/data-protection_en ("In addition, article 16 of the Treaty on the Functioning of the European Union (TFEU) obliges the EU to lay down data protection rules for the processing of personal data. The EU is unique in providing for such an obligation in its constitution").
[41] *Id*. at Article 8.
[42] Council Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 2(c), OJ. L 281/31, at 38 (1995) [hereinafter Directive].
[43] *Id*. at Article 6.
[44] *EU General Data Protection Regulation – Background*, DLA PIPER (2020), https://www.dlapiper.com/en/northamerica/focus/eu-data-protection-regulation/background/.
[45] *See* U.S. LIBRARY OF CONG., ONLINE PRIVACY LAW: EUROPEAN UNION, (updated May 2014), https://www.loc.gov/item/2015296885/.

followed—as shown in Figure 2—the GDPR came into effect almost two decades later as a more stringent version of the Directive.

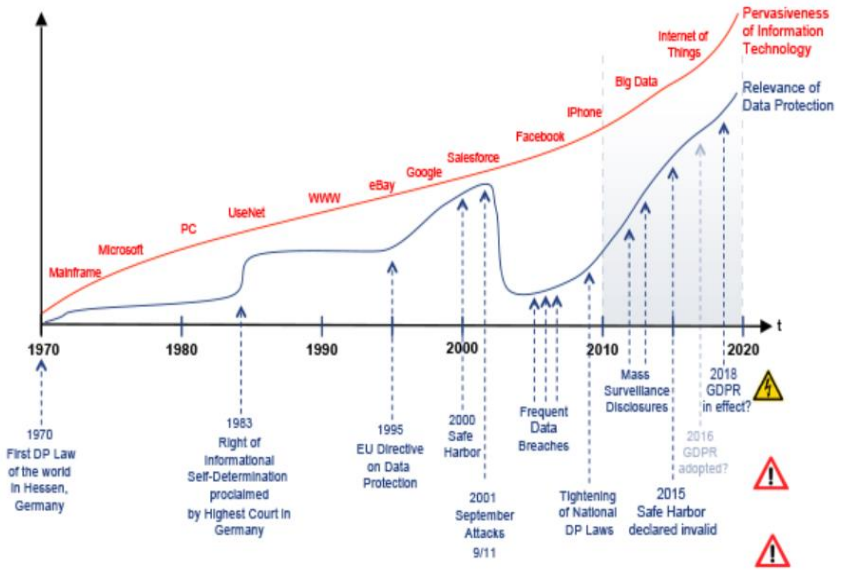

Figure 2. Overview of EU's Data Privacy Legislation (source: IAPP)[46]

[46] *See* Ernst-Oliver Wilhelm, *A Brief History of the General Data Protection Regulation*, INT'L ASS'N OF PRIVACY PROF'L (2021), https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.

2. *The United States' "Patchwork" of Laws*

Similar to the EU, the United States recognizes the right to privacy as a fundamental right. Where the two jurisdictions differ, however, is in the United States' failure to expressly recognize the right to the protection of personal information. Analogous to the European Convention on Human Rights' recognition of the right to privacy, the Fourth Amendment of the United States' Constitution reflects:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[47]

The right to privacy, as it relates to data protection, has closer roots in Tort law than Constitutional law.[48] In the widely cited article by Louis Brandeis and Samuel Warren, the authors identified a fundamental right to "enjoy life . . . the right to be let alone" in the context of the press and media publications.[49] The Restatement (Second) of Torts cites Brandeis' and Warren's article in its expansion of this right to four specific torts (disclosure, intrusion upon seclusion, false light, and appropriation).[50] These rights are mostly based on a reasonableness standard, in which an intentional intrusion on a person's private life and affairs is the standard cause of action.[51] The Restatement states: "whose only relation to one another is that each involves interference with the interest of the individual in leading, to some reasonable extent, a secluded and private life, free from the prying eyes, ears and publications of others."[52] The Restatement's classification reflects how the majority of U.S. courts view this right.[53]

Unlike those of the EU, the principles underpinning the right to privacy in the United States are not uniformly represented throughout data privacy legislation. Instead, its framework consists of "hundreds of state and federal statutes, regulations, binding guidelines, and court created rules regarding data security, privacy, and other issues commonly considered to fall under the umbrella 'cybersecurity.'"[54] At the federal level, the Federal Trade Commission (FTC) is the primary agency responsible for cybersecurity and data privacy

---

[47] U.S. CONST. amend. IV.
[48] *See generally* Leon R. Yankwich, *Right of Privacy: Its Development, Scope and Limitations*, 27 NOTRE DAME L. REV. 499 (1952); Leuan Jolly, *Right of Privacy: Overview, Practical Law Practice Note Overview w-009-4039* (WestLaw). *But see* Harry Kalven Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326 (2012) (discussing tort law's effort to protect the right to privacy as a mistake).
[49] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890); *see also* MULLIGAN *supra* note 2, at 3.
[50] Restatement (Second) of Torts § 652A (1977).
[51] *Id*.
[52] *Id*.
[53] *See generally* Right of Privacy: Overview, Practical Law Practice Note Overview w-009-4039 (WestLaw).
[54] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 NOTRE DAME L. REV. 2211, n.16 (2019).

enforcement across multiple areas.[55] In addition to regulation, the FTC also regularly issues non-binding data privacy security guidelines.[56] In other sectors such as healthcare, the Department of Health and Human Services (HHS) is responsible for regulating data privacy.[57] Under the HIPAA[58] Privacy Rule, HHS "provides comprehensive federal protection for the privacy and confidentiality of IIHI, but generally does not replace federal, state, or other laws that provide individuals even greater privacy protections."[59] Privacy concerns within the healthcare space have increased within the past decade because of the shift to digital record keeping, and COVID-19, among other changes.[60] Other areas of regulation include children's online information,[61] video privacy,[62] and the unauthorized interception of oral and electronic communications.[63]

II. DATA PRIVACY LAWS

Having discussed the development of data privacy in the EU and U.S., this paper now explores the current laws in this space. Specifically, this section will highlight various features of the GDPR, the CCPA and the California Privacy Rights Act, Virginia's Consumer Data Privacy Act, New York Privacy Act, and the Washington Privacy Act.[64] Many of the U.S. state laws analyzed in this paper are either in the process of being enacted, or have been enacted within the past year. As these laws are relatively new, the sources used to analyze these laws are primarily based on non-academic sources such as reports from industry leaders and law firms. This section will discuss each law's purpose, the rights

---

[55] *See* Ieun Jolly, *US Privacy and Data Security Law: Overview, Practical Law Practice Note Overview*, 6-501-4555 (WestLaw).

[56] *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (highlighting best privacy practices); FED. TRADE COMM'N, FEDERAL TRADE COMMISSION STAFF REPORT: SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING: TRACKING, TARGETING, AND TECHNOLOGY (2009), https://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral (recommending how businesses can track individual online activities for advertising); *see also* U. FED. TRADE COMM'N, CROSS-DEVICE TRACKING (2017), https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf (reporting how companies can be transparent in cross-device tracking).

[57] Jolly, *supra* note 55.

[58] Pub. L. No. 104-191 (1996).

[59] *Id*.; *see also* HIPAA Privacy Rule, Practical Law Practice Note 4-501-7220 (WestLaw); *Summary of the HIPAA Security Rule*, U.S. DEP'T. HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html; U.S. DEP'T. HEALTH & HUM. SERV., SUMMARY OF THE HIPAA PRIVACY RULE (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf.

[60] *See, e.g.*, Press Release, OCR Secures $2.175 Million HIPAA Settlement After Hospitals Failed to Properly Notify HHS of a Breach of Unsecured Protected Health Information (Nov. 27, 2019); *see also* Lisa Bari & Daniel P. O'Neill, *Rethinking Patient Data Privacy In The Era Of Digital Health*, HEALTH AFFAIRS (Dec. 12, 2019), https://www.healthaffairs.org/do/10.1377/hblog20191210.216658/full/.

[61] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505.

[62] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.

[63] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522.

[64] Illinois has been very progressive in enacting data privacy laws, but none that are similar to the GDPR/CCPA. The closest legislation was Illinois Data Transparency and Protection Act (SB2330), however, that failed to move forward as of January 2021. As a result, Illinois will not be discussed further in this note. Other states discussed have numerous other privacy laws that will not be discussed; instead, only those laws most similar to the GDPR/CCPA will be.

given to the consumers over their personal data, the types of entities the laws seek to regulate and protect, the enforcement mechanisms, violations, and whether there is a private right of action. This information is organized in Table 1 for further clarity, as well as to lay the groundwork for later discussions regarding the future of U.S. data privacy legislation.

A. *EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION*

The GDPR was developed after years of public consultations, drafts, and legislative amendments, and finally took effect on May 25, 2018.[65] In replacing the EU's Data Protection Directive,[66] the GDPR "set out the rights of individuals and obligations placed on businesses that are subject to the regulation."[67] More specifically, the GDPR's purpose is to "lay down the rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[68] The regulation, which consisted of ninety-nine Articles and a 173-section Preamble, had widespread impact across all EU Member states, individuals, companies, and countries.[69] In fact, the GDPR is considered the "toughest privacy and security law in the world" because of its broad application.[70] To fully understand the impacts the GDPR had on various stakeholders, it is important to understand some of its features, some of which will be highlighted in this section.

The GDPR has set the standard for the types of information protected, as well as the rights consumers have in protecting that information. Personal data is broadly defined by the GDPR as:

> . . .any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[71]

The regulation only applies to "data subjects" who are EU citizens and-or residents.[72] According to the GDPR, these data subjects have the right to access their data,[73] rectify incorrect information,[74] erase or be forgotten,[75] restrict the

---

[65] W. Gregory Voss, *The CCPA and the GDPR Are Not the Same: Why You Should Understand Both*, 1 CPI ANTITRUST CHRONICLE 7-12 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3769825.
[66] Directive, *supra* note 42.
[67] *See* Andrew Rossow, *The Birth of GDPR: What Is It and What You Need to Know*, FORBES (May 25, 2018), https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-ofgdpr-what-is-it-and-what-you-need-to-know/#1d18f7955e5b.
[68] *See* GDPR, *supra* note 6, at art. 1.
[69] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR,* 98 DENVER L. REV. 1 (2020).
[70] *See* Ben Wolford, *What is the GDPR, the EU's new data protection law?*, GDPR.EU (2020), https://gdpr.eu/what-is-gdpr/.
[71] GDPR, *supra* note 6, at art. 4 § 1.
[72] *Id*. at art. 3 § 2.
[73] *Id*. at art. 15.
[74] *Id*. at art. 16.
[75] *Id*. at art. 17.

processing of their data,[76] data portability,[77] object to data collection, and not to be subjected to automated decision-making, including profiling.[78] Significantly, these data subjects have a private right of action that allows individuals to make a claim for material or non-material damage as a result of a breach of these rights.[79]

In enhancing consumers' right to privacy, the GDPR subsequently increased the burden on regulated entities to comply with these rights. The GDPR broadly regulates *any* entity that targets or collects data on data subjects, "regardless of whether the processing takes place in the Union or not."[80] However, the processing of activities must be related to the offering of goods or services to data subjects within the Union.[81] Compliance must be from the "controller" who determines the purposes and means of processing data, and the "processor," who processes the personal data for the controller.[82] Although companies in the United States were initially protected by the EU-U.S. Privacy Shield that alleviated some of the burdens associated with the data protection requirements of the GDPR, the Court of Justice of the European Union declared this shield invalid in 2020.[83]

If any of the regulated entities violate the GDPR, penalties can include administrative fines of up to twenty million euros, or four percent of the total worldwide annual turnover of the previous year.[84] The GDPR has resulted in many violations and fines (see Figure 3). According to the American Bar Association, "a total of 15 EU Member States brought enforcement proceedings that resulted in the issuance of an estimated 91 fines" in 2020, two years after the GDPR's enactment.[85] At the onset of the GDPR's passage, the commission was considerably lax in charges, avoiding imposing the maximum fine with the purpose of "issu[ing] fines in conjunction with corrective measures in what appears to be an attempt to encourage changes in attitude and behavior concerning the protection of personal data."[86] However, multiple fines against global companies were in the tier two level. For example, the Data Protection Authority for Berlin imposed a fine of approximately fourteen million euros on a large German real estate company for serious data retention failings for failing

---

[76] *Id*. at art. 18.
[77] *Id*. at art. 20.
[78] *Id*. at art. 22.
[79] *See* Todd Ehret, *Data privacy and GDPR at one year, a U.S. perspective. Part Two - U.S. challenges ahead*, REUTERS (May 29, 2019, 11:24AM), https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US.
[80] GDPR, *supra* note 6, at art. 3. *See generally* Liane Colonna, *Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?*, 4 INT'L DATA PRIVACY L. 3, 20–221 (2014).
[81] *Id*.
[82] *See* STEPTOE, *California's New Privacy Law: Compliance Guidelines, Comparing the GDPR* 4, https://www.steptoe.com/images/content/1/9/v2/194723/CCPA-Compliance.pdf.
[83] Judgment of 16 July 2020, *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, C-311/18, EU:C:2020:559, in part striking down the Privacy Shield Framework, 81 Fed. Reg. 51,042 (Aug. 2, 2016) and Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, 2016 O.J. (L 207).
[84] STEPTOE, *supra* note 82, at 5.
[85] Catherine Barrett, *Emerging Trends from First Year of EU GDPR Enforcement*, AM. BAR ASS'N (2020), https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/emerging-trends-the-first-year-eu-gdpr-enforcement/#3.
[86] *Id*.

to destroy data for longer than was necessary and denying the right to erasure.[87] Similarly, the French Data Protection Supervisory Authority fined a multinational technology company fifty million euros for breaching GDPR requirements on transparency and consent in relation to personalized advertising.[88]

Figure 3: GDPR Enforcement Actions as of May 25, 2020 (source: DLA Piper)[89]

Figure 3 highlights some of these fines against various entities by EU Member states. Notably, France fined Google upwards of fifty million euros for failing to provide notice in an accessible way and failing to obtain consent to process data for advertisements.[90] The geographical spread of fines, in addition to their sizes, show how important compliance with the GDPR is, effectively resulting in the protection of the fundamental right to privacy of EU citizens.

---

[87] DLA PIPER & AON, THE PRICE OF DATA SECURITY: A GUIDE TO THE INSURABILITY OF GDPR FINES ACROSS EUROPE, 7 (2020), https://www.dlapiper.com/en/uk/insights/publications/2020/05/third-edition-of-guide-on-the-insurability-of-gdpr-fines-across-europe/.
[88] *Id*. at 8.
[89] *Id*. at 5.
[90] HUNTON ANDREW KURTH, *French Highest Administrative Court Upholds 50 Million Euro Fine against Google for Alleged GDPR Violations*, PRIVACY & INFORMATION SECURITY BLOG (2020), https://www.huntonprivacyblog.com/2020/06/23/french-highest-administrative-court-upholds-50-million-euro-fine-against-google-for-alleged-gdpr-violations/.

B. CALIFORNIA CONSUMER PRIVACY ACT AND CALIFORNIA PRIVACY RIGHTS ACT

A few months after the GDPR passed, California enacted its own comprehensive data privacy legislation, the California Consumer Privacy Act,[91] on June 29, 2018. The legislation shares many similar features to the GDPR, some of which will be highlighted in this section.[92] Most notably, the CCPA set precedence as the first U.S. law to address data privacy at the state level as well as provide consumers with rights to access and control their personal information.[93] Similar to the GDPR, the CCPA defines personal information as any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[94] Personal information can include standard identifiers (such as name, email, date of birth, etc.) as well as "less conventional categories such as biometric data, Internet activity, geolocation data, and individual consumer profiles built with other data."[95] The CCPA also provides California residents with similar rights as the GDPR does, including the right to access their personal information, know about the information collected, delete personal information (with some exceptions), opt-out of the sale of their information, and the non-discrimination if they choose to exercise their rights.[96]

The CCPA regulates any entity that conducts business in the state of California and protects California consumer information.[97] Qualification for regulation under the CCPA is determined by various threshold tests, specifically if businesses "either (1) annual gross revenues of $25 million or more; (2) annually buy, receive, sell, or share, for commercial purposes, information from at least 50,000 consumer, households, or devices; or (3) derive at least 50% of their annual revenues from selling consumers' personal information."[98] These businesses can be typically fined up to $750 per incident, if the business faces a data breach, or if the information stolen during a data breach was not reasonably protected.[99] Private rights of action apply to data breaches only, and other actions can be submitted as a complaint to the California Attorney General.[100]

Although largely successful, the CCPA has faced some backlash due to compliance issues, as well as alleged loopholes that allow businesses to escape liability.[101] Even with the California Attorney General's clarification of the law

---

[91] CAL. CIV. CODE § 1798.100—1798.198; For other California privacy laws not discussed in this paper, *see* Online Privacy Protection Act, 2003 CAL. AB 68; Shine the Light Act, CAL. CIV. CODE § 1798.83.
[92] *But see* W. Gregory Voss, *The CCPA and the GDPR Are Not the Same: Why You Should Understand Both*, 1 CPI ANTITRUST CHRONICLE 1, 1 (2021).
[93] *See* Sean Ahern, *First Europe, Now the States: Big Changes Coming to State Data Privacy Laws*, JDSUPRA (June 27, 2018), https://www.jdsupra.com/legalnews/first-europe-now-the-statesbig-changes-36098/.
[94] Cal. Civ. Code § 1798.140 .
[95] STEPTOE, *supra* note 82, at 3.
[96] CAL. CIV. CODE § 1798.100—1798.125.
[97] GIBSON, DUNN & CRUTCHER, *supra* note 15, at 10.
[98] STEPTOE, *supra* note 82, at 4.
[99] *Id*. at 5. *See also* Jeewon Kim Serrato et al., *US States Pass Data Protection Laws on the Heels of the GDPR*, NORTON ROSE FULBRIGHT (July 9, 2018), https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.
[100] *Id*.
[101] *See* Makena Kelly, *California poised to establish a new privacy regulator with ballot measure win*, THE VERGE (Nov. 4, 2020, 12:18PM), https://www.theverge.com/2020/11/4/21549514/california-prop-24-data-privacy-2020-election-andrew-yang.

during various public hearings and draft regulations,[102] critics still hold that the "hastily drafted CCPA presents major compliance challenges for businesses across the country."[103] Others have gone further to say that the CCPA has proven to be a win for consumers but an extreme burden on businesses to implement.[104] Overall, while the CCPA has proven to achieve its goal in increasing consumer rights in the United States, many have found that the law itself is far from perfect.

In response to these shortcomings, over nine million Californians voted to pass Proposition 24, or the California Privacy Rights Act ("CPRA"), in November 2020.[105] This legislation enhances the CCPA, making it even more in line with the GDPR by increasing the rights of consumers as well as adding more variation to the types of information regulation.[106] Most of the law's effects will be implemented by 2023.[107] Additional rights include the right to see all information beyond the past twelve months, correct information, opt out of automated decision-making, and data minimization, to name a few.[108] The law also adds rights to sensitive personal information such as race, religion, genetic, and biometrics.[109] Most significantly, the bill creates an independent data protection agency that removes the exclusive enforcement of the Attorney General.[110] Residents also have the opportunity to bring a private right of action for these new rights.[111] Additional changes include increasing the CCPA "thresholds" for the number of residents, households, or devices businesses collect data from fifty to one hundred thousand.[112] Additionally, businesses that derive fifty percent or more of their annual revenues from selling or sharing consumers' private information are also included.[113]

C. *VIRGINIA CONSUMER DATA PROTECTION ACT*

In March 2021, Virginia became the second state to enact a data privacy law for Virginia residents, the Virginia Consumer Data Protection Act ("CDPA").[114] The legislation grants consumer rights to "access, correct, delete and obtain a copy of personal data and to opt out of the processing of personal data for the

---

[102] *See* GIBSON, DUNN, & CRUTCHER, *supra* note 97, at n.50.
[103] *See California AG Faces Criticism of Draft Regulations at Los Angeles CCPA Hearing*, WILEY (2019), https://www.wiley.law/alert-California_AG_Faces_Criticism_of_Draft_Regulations_at_Los_Angeles_CCPA_Hearing.
[104] Michael Fertik, *CCPA Is a Win For Consumers, But Businesses Must Now Step Up on CX,* FORBES (Jan. 27, 2020, 5:40PM), https://www.forbes.com/sites/michaelfertik/2020/01/27/ccpa-is-a-win-for-consumers-but-businesses-must-now-step-up-on-cx/?sh=7c752b426557.
[105] *See generally California Privacy Rights Act Executive Summary*, Californians for Consumer Privacy Committee, https://www.caprivacy.org/cpra-exec-summary/.
[106] *Id*.
[107] *Id*.
[108] *Id*.
[109] *Id*.
[110] *Id*.
[111] *Id*.
[112] *See CPRA vs. CCPA vs. GDPR: How the Difference Impacts Your Data Privacy Operations*, WIREWHEEL 2 (2021), https://wirewheel.io/wp-content/uploads/2020/11/WireWheel-GDPR-vs-CCPA-vs-CPRA-Cheat-Sheet.pdf.
[113] *Id*.
[114] Sten-Erik Hoidal & Megan A. Bowman, *Virginia Becomes Second State to Pass Comprehensive Consumer Privacy Law*, FREDRIKSON & BYRON, P.A. (Mar. 16, 2021) https://www.fredlaw.com/news__media/virginia-becomes-second-state-to-pass-comprehensive-consumer-privacy-law/.

purposes of targeted advertising."[115] Personal data includes the typical identifiable information, as well as sensitive information similarly protected by the CCPR (such as geographic location, race, and biometric data).[116] Unlike the GDPR and CCPA-CCPR, however, the CDPA does not give residents a private right of action.[117]

The CDPA poses similar burdens on businesses to comply with the protection of personal information as other data privacy laws. It applies to any person that conducts business in Virginia, or produces products or services targeted to residents of Virginia, "and that (i) during a calendar year, control or process personal data of at least 100,000 consumers or (ii) control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data."[118] These threshold tests are similar to the new amendments proposed by the CCPR for California. The penalties are the same as the CCPR, as well as any violation of the chapter can cost up to $7,500 for each violation.[119] Where the CDPA differs is in its enforcement: Virginia takes a hybrid approach by allowing the Attorney General to have exclusive enforcement authority, as well as the Consumer Privacy Fund that collects the penalty fees.[120]

D. *NEW YORK PRIVACY ACT*

The New York Privacy Act[121] is a culmination of numerous attempts by New York to pass a data privacy law similar to the CCPA-CCPR and CDPA.[122] A previous iteration of the bill did not pass the previous legislative session due to COVID-19 priorities,[123] however, many commentators are hopeful that the current draft will have more luck given the new administration.[124] Compared to the other data privacy laws, the legislation tends to give consumers more rights. For example, personal information includes any "information relating to an identified or identifiable natural person."[125] In addition to the Attorney General who can bring an action on behalf of private persons with the help of a privacy fund, the Act also includes an expansive private right of action:

---

[115] *Id*.
[116] *Id*. at § 59.1-571.
[117] *Id*. at § 59.1-580.
[118] *Id*. at § 59.1-572.
[119] *Id*. at § 59.1-580.
[120] *Id*. at § 59.1-581.
[121] New York Privacy Act, N.Y. Gen. Bus. Law. §§1100–1110 (2021), https://www.nysenate.gov/legislation/bills/2021/A680..
[122] *See generally* Mylan Denerstein et al,. *Prepare For NY Data Privacy Law To Catch Up To Calif.*, GIBSON, DUNN, & CRUTCHER (2021), https://www.gibsondunn.com/wp-content/uploads/2021/02/Denerstein-Southwell-Aycock-Prepare-For-NY-Data-Privacy-Law-To-Catch-Up-To-Calif.-Law360-01-29-2021.pdf (highlighting recent New York legislative developments as of January 2021).
[123] Viola Trebicka et al., *Inside the Proposed New York Privacy Act*, THE N.Y. L.J., (Sept. 2, 2020, 11:21AM), https://www.law.com/newyorklawjournal/2020/09/02/inside-the-proposed-new-york-privacy-act/.
[124] Klein Moynihan Turco, *NY Assembly Reintroduces NY Privacy Law*, LEXOLOGY (Jan. 19, 2021), https://www.lexology.com/library/detail.aspx?g=b21e5ad8-c8f5-4a41-ade7-7a34d5077a12.
[125] New York Privacy Act, *supra* note 121, at § 1100(10).

> [A]ny person who has been injured by reason of a violation of this article may bring an action in his or her own name to enjoin such unlawful act, or to recover his or her actual damages, or both such actions. The court may award reasonable attorney's fees to a prevailing plaintiff.[126]

Consumer rights include the right to opt in or opt out of processing their data and consent,[127] correction,[128] deletion of data (with exceptions)[129] restriction of processing if certain conditions are met,[130] and portability.[131]

The New York Privacy Act is comparatively more onerous for regulated businesses than other current data privacy legislation. Legal entities include those that conduct business in New York state, "or produce products or services that are intentionally targeted to residents of New York State."[132] Unlike the CCPA-CCPR and the CDPA, there are no threshold tests to determine who constitutes a business, or minimum amounts of personal data that must be processed.[133] Furthermore, the fine is determined on a case-by-case basis, and can result in an injunction, damages, and a civil penalty. Factors considered include the severity of the violation, the revenue of the entity, and number of affected individuals.[134]

E. *WASHINGTON PRIVACY ACT*

Similar to New York, Washington State has repeatedly attempted to pass a data privacy law. The Washington Privacy Act[135] goes further than these laws in its purpose, highlighting privacy "as a fundamental right and an essential element of [Washington Resident's] individual freedom."[136] In protecting this right, this law will give consumers the "right to access, correct, and delete personal data, as well as the rights to obtain data in a portable format and to opt out of the collection and use of personal data for certain purposes."[137] It applies the same standard language regarding jurisdiction, such as monitoring all legal entities doing business in Washington that control or process over one hundred thousand consumers, and derives over twenty-five percent of gross income from the sale of personal data.[138] Although there is no private right of action, the Act is enforceable by the Attorney General, who upon taking various actions can fine the entity a civil penalty of up to $7,500 for each violation.[139]

---

[126] *Id*. at § 1109(3).
[127] *Id*. at § 1103.
[128] *Id*. at § 1103(2).
[129] *Id*. at § 1103(3).
[130] *Id*. at § 1103(35).
[131] *Id*. at § 1103(8)(b).
[132] *Id*. at § 1101.
[133] Kyle Fath & Melinda McLellan, *New York Legislature Introduces CCPA Clone with Private Right of Action*, JD SUPRA (Jan. 8, 2021), https://www.jdsupra.com/legalnews/new-york-legislature-introduces-ccpa-6501577/.
[134] New York Privacy Act, *supra* note 121, at § 1109.
[135] Washington Privacy Act (Washington SB. 5062), http://lawfilesext.leg.wa.gov/biennium/2021-22/Pdf/Bills/Senate%20Bills/5062-S.pdf?q=20210125113540.
[136] *Id*.
[137] *Id*. at § 2.
[138] *Id*. at § 102.
[139] *Id*. at § 112. Also notable are the costs of investigation, including reasonable attorneys' fees.

F. *SYNTHESIS*

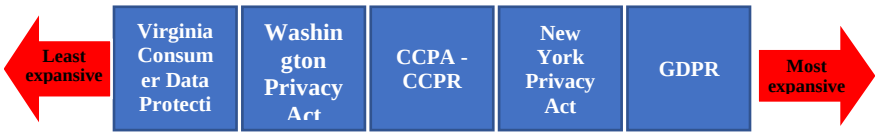

Figure 4. Continuum of Data Privacy Laws

This section summarized key features of leading data privacy laws from the EU and U.S. states. Overall, the U.S. laws bear close similarities to the GDPR, with slight variations. These variations allow these laws to be placed on a continuum (see Figure 4) that takes into account the rights given to the consumers, the extent of regulation (e.g., fifty versus one hundred thousand consumers), as well as its level of enforcement. The extent of regulation is the biggest difference amongst these laws, and therefore dictates where these laws sit on the spectrum. On the right, the GDPR is the most expansive because it applies to any entity that targets or collects data, without any threshold tests. The New York Privacy Act closely follows as it similarly lacks any threshold tests. The Washington Privacy act is slightly less expansive than the CCPA-CCPR because the latter provides a private right of action. Virginia CDPA is the left-most law because it requires a higher threshold for the total amount of gross revenue required for regulation (fifty percent compared to twenty-five percent in the CCPA-CCPR). Overall, an analysis of these laws shows numerous similarities, and provides a solid foundation for what can make up the future U.S. data privacy law.

III. TABLE 1. SIDE-BY-SIDE DATA PRIVACY LAW MATRIX

	GDPR	CCPA (as modified by the CCPR)	Virginia Consumer Data Protection	New York Privacy Act	Washington Privacy Act
Citation	Commission Regulation 2016/679, 2016 O.J. (L 119) (EU)	Cal. Civ. Code § 1798.100—1798.198.	Va. Code Ann. § 59.1-571—59.1.1-581	New York Privacy Act, 2021, N.Y. Gen. Bus. Law. §§1100 – 1110	Washington Privacy Act (Washington SB. 5062)
Purpose of the Law	To protect natural persons with regard to the processing of personal data and lay down the rules relating to the free movement of personal data	Provide consumer rights to "request that a business that collects a consumer's personal information disclose to that consumer the categories and specific pieces of personal information the business has collected" (§ 1798.140(a)).	"Establishes a framework for controlling and processing personal data in the Commonwealth"	"Enacts the NY privacy act to require companies to disclose their methods of de-identifying personal information, to place special safeguards around data sharing and to allow consumers to obtain the names of all entities with whom their information is shared; creates a special account to fund a new office of privacy and data protection."	Protect the fundamental right to privacy, an essential element of Washington residents' freedom.
Who is Regulated?	Any entity that targets or collects data on data subjects	Businesses collecting data from 100k households, or derives 50% of revenue from selling personal information	Businesses processing personal data of 100k consumers or businesses that control or process personal data of at least 25k consumers; or derive 50% revenue from the sale of personal data	Legal entities that conduct business in New York state, or produce products or services that are intentionally targeted to residents of New York state	Legal entities that conduct business in Washington, or produce products or services that are targeted to residents of Washington, and (1) control or possess data of 100k or more consumers; (2) derives 25% of gross revenue from the sale of personal data

Who is Protected?	EU citizens and residents	Natural person who is a resident of California.	". . .natural person who is a resident of the Commonwealth acting only in an individual or household context"	Natural person who is a New York resident	Resident acting in household or individual context
Rights	Access; Rectify; Erasure; Restriction of Processing; Data Portability; Object; Not to be Subjected to Automated Decision-making	Know about the information collected; Delete (with some exceptions); Correct; Opt-out of the sale of information and automated Decision-making; Portability; and Non-discrimination	Access; Correct; Delete; Obtain a copy of personal data; Opt-out of the processing of personal data for the purposes of targeted advertising	Opt-in or opt-out of processing their data and consent; Correction; Deletion of data (with exceptions); Restriction of processing if certain conditions are met; Portability	Access; Correct; Delete Obtain data in a portable format; Opt-out of the collection and use of personal data for certain purposes
Private Right of Action?	Yes	Yes, for data breaches only	No	Yes	No
Enforcement	European Data Protection Board	Attorney General (CCPA); California Privacy Protection Agency	Attorney General and Consumer Privacy Fund	Attorney General and privacy fund	Attorney General
Violations	Administrative fines of up to €20 million, or 4% of the total worldwide annual turnover of the previous year	Penalties range from $2,500 for a nonintentional violation to $7,500 for an intentional violation. CCPR increases fines to $7,500 for each violation of CPRA involving personal information of consumers under the age of 16.	Up to $7,500 for each violation.	Injunction and damages for a civil penalty; includes number of affected individuals, severity of the violation, and size of revenue of the entity	Up to $7,500 for each violation

IV. ANALYSIS: POTENTIAL CONSIDERATIONS FOR FUTURE U.S. DATA PRIVACY

A. *WHY THERE NEEDS TO BE A COMPREHENSIVE U.S. FEDERAL DATA PRIVACY LAW*

As this Note has highlighted, many U.S. states as well as the EU have made noteworthy progress in creating legislation that provides consumers comprehensive rights over their personal information within the past few years. However, as the various "patchwork" of state laws increase, the need for a federal U.S. privacy legislation remains a popular but challenging goal.[140] There are two reasons why federal reform is needed. First, the industry would benefit from a uniform standard because it would provide a more streamlined approach to data privacy. Such a standard can result in clarity for both the regulated entities, as well as those designated to enforce the law. As shown in this Note, state laws are too varied in their requirements (such as the threshold tests), subsequently creating additional burdens on businesses to comply with each state separately. Second, a comprehensive data privacy legislation will give consumers uniform rights over their personal information. As more consumers become aware of how their personal data—including sensitive information—is sold for profit through other comprehensive laws such as the GDPR, their interest in protecting their rights will increase as well.[141] This section summarizes these arguments, as well as provides a normative discussion on potential features that can be included in a federal data privacy legislation such as uniform consumer rights, federal and state partnerships for enforcement, and the inclusion of a private right of action.

1. Industry Benefit

The industry would benefit from a comprehensive data privacy law because it would increase clarity for both the regulated entities as well as those designated to enforce the law. This clarity can have positive effects, such as the opportunity to compete fairly and effectively in the global economy. Technology companies like Google, Twitter, and Facebook have expressed and urged the need for a federal data privacy law.[142] Past federal legislative attempts supporting data privacy reform reflect these views.[143] For example, in her testimony to the U.S. Senate Committee on Commerce, Science, & Transportation, Julie Brill—the current Chief Privacy Officer of Microsoft—

---

[140] *See generally* GIBSON, DUNN & CRUTCHER, *supra* note 15.

[141] Karen Schuler, *Federal data privacy regulation is on the way — That's a good thing*, INT'L ASS'N OF PRIV. PRO. (Jan. 22, 2021), https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/#:~:text=Various%20federal%20laws%20%E2%80%94%20including%20the,%2C%20patients%2C%20minors%20and%20others.

[142] *See, e.g.*, *Google, Twitter, Amazon hope for US data privacy law*, DECCAN HERALD (Jan. 13, 2021, 6:01 PM), https://www.deccanherald.com/business/business-news/google-twitter-amazon-hope-for-us-data-privacy-law-938632.html.

[143] *See, e.g.*, "Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act" or the "SAFE DATA Act;" S. 2968, the "Consumer Online Privacy Rights Act" or "COPRA;" and S. 3456, the "Consumer Data Privacy and Security Act of 2020."

testified regarding the need for comprehensive reform. [144] In her testimony, she states:

> What has not changed is the urgent need to pass a comprehensive privacy law. In December, I said that a comprehensive privacy law was more urgently needed than ever before. What was merely urgent 10 months ago is absolutely critical now. The degree to which we can come together as a nation to end the coronavirus public health crisis; build a sustainable recovery; and address systemic racism in our society will depend in part on how well and responsibly we use the data that today's digital systems enable us to collect. We would be much better able to responsibly harness data to address the greatest issues of our time if we had a national comprehensive privacy law in place.[145]

Julie Brill's sentiment is shared by other Chief Privacy Officers as well. In an interview with IBM's Chief Privacy Officer, Christina Montgomery, Montgomery states: ". . .I'm hopeful that we do [have a federal data privacy law]. We've long been advocating for a national privacy law."[146] Overall, the industry has overwhelmingly expressed support for this type of legislation.

At the same time, a federal data privacy law can disproportionately affect smaller businesses not equipped to deal with even the most basic requirements.[147] Unlike the big-technology companies, such as Google and Microsoft, that have the resources to adapt to a federal data privacy law, small businesses (the remaining ninety-nine percent of all businesses)[148] might not. Challenges associated with a COVID-19 economy, including supporting employees, changes in customer preferences, and reduced demand make privacy concerns a secondary priority.[149] Coupled with the potential costs (such as legal fees) associated with adapting to federal data privacy standards, this law could actually be more burdensome on these small businesses than the status quo. However, as states are adapting their own data privacy laws, the burden may not be as demanding if the federal data privacy law adapts similar features as specified in these laws.[150] The federal law's recognition of the current state laws

---

[144] *Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the Committee on Commerce, Science, & Transportation U.S. Senate*, 116th Cong. 2-3 (2020) (statement of Julie Brill, Corporate Vice President, Chief Privacy Officer, and Deputy General Counsel for Global Privacy and Regulatory Affairs, Microsoft Corporation).

[145] *Id*. at 2.

[146] *See* Frank Ready, *IBM's Chief Privacy Officer Talks Federal Privacy Legislation as Antidote to Tech Mistrust*, LAW.COM, (Feb. 1, 2021, 7:00 AM), https://www.law.com/legaltechnews/2021/02/01/ibms-chief-privacy-officer-talks-federal-privacy-legislation-as-antidote-to-tech-mistrust/.

[147] *See, e.g.*, Paula Bruening, *Crafting a Federal Privacy Law to Benefit Small Businesses*, BLOOMBERG LAW (Oct. 5, 2020, 4:01 AM), https://news.bloomberglaw.com/us-law-week/crafting-a-federal-privacy-law-to-benefit-small-businesses.

[148] U.S. SMALL BUS. ADMIN., *2020 Small Business Profile*, Office of Advocacy (2020).

[149] *Id*.

[150] *See* Eric Goldman, *What we've learned from California's Consumer Privacy Act so far*, THE HILL (Jan. 11, 2020, 2:00 PM), https://thehill.com/opinion/cybersecurity/477821-what-weve-learned-from-the-california-consumer-privacy-act-so-far (reporting that "[t]he DOJ estimates that CCPA will affect between 15,000 and 400,000 businesses—a startlingly wide range. The DOJ also estimates that 'up to 50 percent' of the affected businesses will be 'small' businesses, even though CCPA's authors sought to exclude small businesses from its scope").

will make it easy for both the state and the business to enhance consumer privacy rights.

2. *Consumer Rights*

A comprehensive data privacy legislation can provide all U.S. citizens and residents uniform rights over their personal information. Americans value their right to privacy, as shown by California's Proposition 24 initiative that garnered over nine million supporters, as well as a recent KPMG study that found consumers view data privacy as a human right.[151] Federal agencies, such as the FTC, have similarly supported this type of legislation with the goal of upholding consumer rights.[152] For example, the former Commissioner and Chair of the Federal Trade Commission argued for a federal data privacy law because "Americans across the country would be protected by the same consistent privacy regime regardless of where in the United States they live, work, or happen to be accessing information. Consumers in every state would have far more control of their own data."[153] Instead of only California and Virginia residents bearing entitlement to this protection, all citizens would at least be given the choice to consent to the data that entities make an enormous profit from through a federal regulation.

Businesses against a uniform data privacy law may argue that consumers accept the status quo, because it gives them a more personalized experience. For example, Google's privacy policy states that it collects data to "build better services"[154] that include personalized content, relevant recommendations, and customized search results. According to the same KPMG study, "To a large degree, consumers have been okay with this. They know it can make for a better shopping experience, enabling things like quick reordering of favorite items and express checkout with saved payment information."[155] However, a federal legislation would not remove this level of personalization for the consumer. The right to consent or opt-in to data sharing allows customers the choice to participate in the businesses' use of their data. Without this choice, Americans are being denied a fundamental right to privacy promised in American jurisprudence. Additionally, a federal data privacy legislation would ensure the data is secured and protected from data breaches, which might result in the information being shared with adverse third parties. As the Attorney General of California stated in a legislative hearing: "On a broader level, if businesses want to use consumers' data, they should have a duty to protect and secure it, and wherever feasible, minimize data collection. Businesses should no longer approach consumer data with the mindset, 'collect now, monetize later.'"[156]

---

[151] California Attorney General, *supra* note 105; *see* Orson Lucas & Steven Stein, *The New Imperative For Corporate Data Responsibility*, KPMG (2020),

[152] *Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the U.S. Senate Committee on Commerce, Science, & Transportation* 116th Cong. 7 (2020) (statement of Jon Leibowitz, Former Commissioner and Chair, Federal Trade Commission).

[153] *Id*. at 3.

[154] *See* Google Privacy & Terms, https://policies.google.com/privacy?hl=en&fg=1#whycollect.

[155] Lucas & Stein, *supra* note 151.

[156] *Revisiting the Need for Federal Data Privacy Legislation: Hearing Before the U.S. Senate Committee on Commerce, Science, & Transportation* 116th Cong. 5 (2020) (statement of Xavier Becerra, Attorney General of California).

B. *POTENTIAL FACTORS TO CONSIDER: A NORMATIVE POLICY DISCUSSION*

1. *Uniform Consumer Rights*

Based on the various laws analyzed in this Note, a U.S. federal data privacy law should consist of a strong set of uniform consumer rights that are applied to consumers (all U.S. citizens and legal residents). Currently, entities are required to provide consumers different rights based on where they live. For the states that have already considered or already passed data privacy laws, these rights typically include the right to access, delete, and obtain personal information, as well as consent for both sensitive and non-sensitive information, data portability, and the right to opt-out of processing personal data for targeted advertising.[157] It is practical neither for consumers to expect to have different rights depending on where they access the internet or other technology, nor for businesses to comply with different regulatory standards by states. At a minimum, the common rights enumerated above should be considered in a federal legislation.

2. *Federal and State Partnerships for Enforcement*

Congress should consider creating an entirely new structure, such as a data privacy office within an already existing agency, that is designed to help businesses and consumers resolve complaints. This agency would likely reside within the FTC, and can work closely with state attorney generals to set determine appropriate policies. Working with state attorney generals would benefit states that have already enacted a data privacy legislation, and would potentially overcome issues of preemption. Overall, companies need a resource that can provide them clear guidance on how to amend their business operations to be in compliance with the federal data privacy law. Having an office dedicated to this purpose would alleviate any burdens on businesses as well as provide direct and clear communication to consumers.

3. *Private Right of Action*

Lastly, absent another office that can enforce the federal law, Congress should consider including a private right of action for citizens to bring their claims. A private right of action would allow individuals to sue companies directly of violations of their rights to privacy, as is included in the GDPR, CCPA-CCPR, and the New York Privacy Act. Without this option, enforcement is left to the state and federal enforcement agencies like the FTC and other privacy funds and offices advocated by the states.[158] Although data privacy is a bipartisan issue, the inclusion of the private right of action tends to become a political issue. According to a recent Gibson Dunn report, "Democratic

---

[157] See Table 1 for a summary of these rights.

[158] Becky Chao, Eric Null & Claire Park, *A Private Right of Action is Key to Ensuring that Consumers Have Their Own Avenue for Redress*, NEW AMERICA (Nov. 20, 2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/a-private-right-of-action-is-key-to-ensuring-that-consumers-have-their-own-avenue-for-redress/#:~:text=With%20a%20private%20right%20of,sue%20the%20violating%20company%20directly.&text=For%20example%2C%20under%20tort%20law,assault%2C%20battery%2C%20or%20trespassing.

legislators, in general, favor federal privacy legislation that includes a private right of action, while Republicans tend to favor legislation that explicitly preempts state privacy laws.[159] However, Congress may be able to draft the law in such a way that can be both enforced by agencies as well as by individuals through a private right of action. For example, California allows for a private right of action pertaining to data breaches only; all other claims are handled by its state Attorney General. While there are definite pros and cons to including a private right of action, it should strongly be considered in future regulations.

CONCLUSION

In sum, the United States should consider passing a federal data privacy law in order to increase consumer rights as well as alleviate inconsistencies that face businesses grappling with various state laws. Without federal guidance, American's right to privacy is jeopardized, and companies have to adapt to various state laws that impose different requirements for compliance. The GDPR was the first law of its kind to balance the right to privacy with the advent and creation of new technology. The law set a clear baseline for how companies should manage personal information, and the United States should not shy away from doing the same. While efforts from California and Virginia are steps in the right direction, there is still much more to be done in recognizing consumers' fundamental right to privacy.

[159] GIBSON, DUNN & CRUTCHER, *supra* note 15, at 15.