Cybaris®

Volume 10 | Issue 1 Article 2

2019

# Creating a National Data Privacy Law for the United States

Shaun G. Jamison

# CREATING A NATIONAL DATA PRIVACY LAW FOR THE UNITED STATES

BY SHAUN G. JAMISON[1]

TABLE OF CONTENTS



[1] The author's biographical information can be found on Linkedin at: https://www.linkedin.com/in/shaunjamison/.

## I. INTRODUCTION

The United States (U.S.) lacks a cohesive data privacy law.[2] This article will examine the need for a national data privacy law, challenges to creating a national privacy law, and possible paths forward to a national privacy law. Presently, U.S. law is a combination of federal sectoral laws and state laws. This myriad of laws makes compliance for interstate and international companies difficult, expensive, and arguably, unattainable. Further, with the European Union's (E.U.) adoption of the General Data Protection Regulation (GDPR),[3] many U.S. companies already have to comply with the GDPR due to doing business or having data processed in the E.U.[4] Japan has entered into an agreement with the E.U. recognizing the equivalency of each other's privacy laws.[5] The U.S. must update its laws to avoid risking limiting its access to markets where countries have modernized their privacy laws. Indeed, California passed a sweeping privacy law which will be effective in 2020, creating more urgency to the issue.[6] The size of California's economy threatens to make their law de facto national law.[7] Because the law affects companies' wishes to

---

2 Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN RELATIONS (January 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection.

3 *E.U. General Data Protection Regulation (GDPR): Regulation (E.U.) 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)*, 2009 O.J. (L 119) 1. (hereinafter GDPR).

4 Matthias Artzt, *Territorial scope of the GDPR from a US perspective*, IAPP: THE PRIVACY ADVISOR (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/.

5 *International data flows: Commission launches the adoption of its adequacy decision on Japan*, EUROPEAN COMMISSION (September 5, 2018), http://europa.eu/rapid/press-release_IP-18-5433_en.htm.

6 Tal Kopan, *California law could be Congress' model for data privacy. Or it could be erased*, SAN FRANCISCO CHRONICLE (Feb. 10, 2019), https://www.sfchronicle.com/politics/article/California-law-could-be-Congress-model-for-13604213.php.

7 Dipayan Ghosh, *What You Need to Know About California's New Data Privacy Law*, HARVARD BUSINESS REVIEW (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law.

do business with California residents, many national companies will likely choose to comply rather than forego access to California's large population and economy.

One of the main challenges to a national data privacy law is the United States' system of federalism. States have been seen as laboratories for policy experimentation.[8] Powers not given to the federal government are reserved to the states and the people.[9] Federal law must rely on express delegation of authority by the Constitution or via application of the Commerce Clause.[10] As civil cybersecurity and privacy are not addressed in the U.S. Constitution, the federal government must rely on the Commerce Clause. While the Commerce Clause may ultimately be successful as grounds for a national law, one can anticipate states to resist any preemption of their existing data privacy laws. A further challenge is creating the "political will" to create a national data privacy law.

The White House set forth its cybersecurity policy,[11] and while it does not advance a national data privacy law, it does not preclude it. While a uniform law throughout the U.S. is appealing to industry, Congress could pass a law which does not preempt additional protections by states. This would remove the threat of lawsuits by states which feel their laws do a better job of protecting consumers than a proposed federal law. However, any law sufficient enough to gain adequacy ruling from the E.U. can be argued to appropriately protect consumers and thus it is not

---

[8] Harry N. Scheiber, *Federalism and the Process of Governance in Hurst's Legal History*, 18 LAW & HIST. REV. 205, 206 (2000).

[9] U.S. Const. amend. X states: "The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people."

[10] "The Congress shall have Power . . . To regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes." U.S. Const. Art. I, § 8, cl. 3.

[11] Grant Schneider, *President Trump Unveils America's First Cybersecurity Strategy in 15 Years*, WHITEHOUSE.GOV (September 20, 2018), https://www.whitehouse.gov/articles/president-trump-unveils-americas-first-cybersecurity-strategy-15-years/.

necessary to retain all of the provisions of existing state laws. Naturally, this is not an uncontested viewpoint. A further challenge is that technology companies would be reticent to throw their support behind a national law that does not preempt state law as it leaves them exposed to complying with a complex web of state laws.[12] Despite the obstacles, there is more to gain with a cohesive regulatory structure than the obstacles and risks to enacting one.

## II. THE NEED FOR A NATIONAL DATA PRIVACY LAW

### A. WHAT IS DATA PRIVACY?

Data privacy, otherwise known as information privacy, is the right to have control[13] and knowledge about any personally identifiable information (PII) which is collected about an individual. Definitions of what constitutes PII vary. Sometimes a combination of bits of information can make it personally identifiable. Certainly, the combination of your name with your social security number or bank account number fits the definition. With access to information such as this, someone could open accounts in your name and access even more information about you than they already had. NIST, the National Institute of Science and Technology, defines PII as:

> Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).[14]

---

[12] David Shepardson, *Tech companies back U.S. privacy law if it preempts California's*, REUTERS (September 26, 2018), https://www.reuters.com/article/us-usa-tech-congress/tech-companies-back-u-s-privacy-law-if-it-preempts-californias-idUSKCN1M62TE.

[13] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1089 (2006).

[14] National Institute of Standards and Technology Glossary (Retrieved March 12, 2019 from https://csrc.nist.gov/glossary/term/PII).

Medical diagnoses are rightly considered private information and can lead to serious consequences if revealed such as adverse employment actions, damage to reputation, and conflict with family members. Personal Health Information is known as PHI. PHI is defined as:

> All individually identifiable health information that is transmitted electronically, maintained in any electronic medium, or transmitted or maintained in any other form or medium. This information has been created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates to the past, present and future physical and mental health, provision of health care to the patient and payment for the patient's health care.[15]

### B. WHAT IS THE DIFFERENCE BETWEEN PRIVACY & CYBERSECURITY?

It is important to note here that it is easy to conflate privacy with cybersecurity because the two are so closely linked. Privacy has to do with the collection, storage, and dissemination of personal information. Cybersecurity is the protection of systems from intrusion. This may involve personal data, proprietary data, and control of systems or connected devices. How they interconnect is that ineffective cybersecurity practices can expose personal data and allow access by unauthorized persons to that data. Further, proper privacy policies and procedures may eliminate the risk by making sure that unneeded sensitive personal information is either never collected in the first place or that it is effectively destroyed when no longer needed. You cannot have a privacy breach for information you do not have. Finally, there is a third aspect of the discussion which is breach notification. Despite best efforts, an organization may have a privacy or cybersecurity breach. If so, there are presently many different laws they potentially need to comply with as far as notifying potentially affected parties, regulators, and sometimes the media of the breach. This paper will focus on privacy and breach notification.

---

[15] D'Arcy Guerin Gue and Steven J. Fox, *Guide to Medical Privacy and HIPAA Appendix III*. (Thompson Information Services 2015).

### C. PRIVACY LAWS ARE A PATCHWORK OF STATE & FEDERAL LAWS

A brief overview of some of the current laws in place will help put the problem in context. The fact that some areas of data privacy may have fifty-one laws makes it challenging to comply and confusing for consumers. Additionally, many will argue there are gaps in the current framework. Further, the "U.S. is one of the few countries in the developed world without a national privacy law or a watchdog dedicated to consumer data."[16]

#### 1. THE FTC ACT

The Federal Trade Commission (FTC) is the leading federal agency addressing privacy issues in the U.S. The FTC derives its authority in this area from the FTC Act, in particular section 45(a) which addresses unfair or deceptive trade practices.[17] Unfair practices are unlawful: "unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[18] In order to act, the FTC must show that the unfair activity:

1. Is causing or likely will cause substantial harm to consumers,
2. Is not reasonably avoidable by the consumers, and
3. Is not outweighed by the need to compete or the benefits to customers.[19]

---

16 Emily Birnbaum & Harper Neidig, *State Rules Complicate Push for Federal Data Privacy Law*, THE HILL (March 5, 2019), https://thehill.com/policy/technology/432564-state-rules-complicate-push-for-federal-data-privacy-law.

17 15 U.S.C. § 45.

18 *Id*. at (a)(1).

19 *Id*. at (n).

The FTC's authority to act on privacy was unsuccessfully challenged in *F.T.C. v. Wyndham Worldwide Corp*.[20] The FTC's authority is broad and flexible and applies to both cybersecurity and misleading privacy policies.[21]

The FTC currently does not use broad rulemaking authority and organizations rely on a common law of FTC enforcement actions as guidelines.[22] The FTC also publishes guides, such as *Start with Security: A Guide for Business*.[23] Further, the FTC does not levy fines immediately on privacy enforcement actions. They first negotiate a consent order, and if they are unable to do so, then litigate against an organization.[24] The ability to fine an organization at the beginning could be an effective deterrent.

### 2. COPPA

The Children's Online Privacy Protection Act (COPPA) was passed in 1998.[25] COPPA requires that sites which gather private information on children under the age of thirteen must follow certain rules. For example, any gathering of personally identifiable information (PII) of a child under thirteen years of age requires "verifiable parental consent."[26] No more information will be gathered than necessary and the child's participation in a game will not be conditioned

---

[20] F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 249 (3d Cir. 2015).

[21] *See Id.*

[22] *See* Michael Scully & Cobun Keegan, *IAPP Guide to FTC Privacy Enforcement*, IAPP, https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf (last visited Mar. 12, 2019).

[23] *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[24] *See* Michael Scully & Cobun Keegan, *IAPP Guide to FTC Privacy Enforcement*, IAPP, https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf (last visited Mar. 12, 2019).

[25] 15 U.S.C. § 6501.

[26] 15 U.S.C. § 6502 (b)(1)(A)(ii).

upon giving personal information.[27] Further, the website must give notice "of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information."[28]

### 3. GLBA

The Gramm Leach Bliley Act (GLBA) specifically addresses privacy within financial institutions.[29] The policy behind this is: "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[30] One of the goals of the GLBA is to address the issue of identity theft which has been described above.[31]

The GLBA relies on an "opt out" procedure for nonpublic personal information. The financial institution may disclose they will share information[32] and then the consumer has the option to notify the financial institution that they do not wish to have their information shared.[33] Despite the heightened attention that privacy has received of late, people generally do not read these notices and thus are not likely to protect their rights by opting out.[34]

---

[27] 15 U.S.C. §6502 (b)(1)(C). Requiring consent prior to gathering information is referred to as "opt in." "Opt out" meaning an organization can act until consent is withdrawn.

[28] 15 U.S.C. § 6502 (b)(1)(A)(i).

[29] 15 U.S.C. § 6801.

[30] 15 U.S.C. § 6801(a).

[31] R. Bradley McMahon, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 627 (2004).

[32] 15 U.S.C. § 6802(b)(1)(A).

[33] 15 U.S.C. § 6802(b)(1)(B).

[34] Of the respondents to one survey about how often they read a privacy notice, the results were: "never (16.2%) or rarely (43%) read privacy policies. Another 32.1% suggest that they "sometimes" read privacy notices. Fewer than 9% of respondents do so "always" or "often." Ari Ezra Waldman, *A Statistical Analysis of Privacy Policy Design*, 93 NOTRE DAME L. REV. ONLINE 159, 166 (2018).

### 4. HIPAA

Like the GLBA, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[35] is a sectoral law. However, it is focused on the healthcare industry rather than the financial. HIPAA provides guidance on providing notice, protecting personal health information (PHI), and proper release of PHI. Release of PHI information not otherwise authorized must be authorized by the patient in writing.[36] As you can imagine, health information is considered highly sensitive. HIPAA also provides patients with a broad right of access to their information with certain exceptions.[37] Courts have ruled there is no private right of action for violation of HIPAA.[38]

### 5. FERPA

The Family Educational Rights and Privacy Act (FERPA)[39] addresses the privacy of student records. Unlike some of the other laws, it does not address cybersecurity law directly. It protects student records against disclosure.[40] Once a student turns eighteen years of age, the parents lose access to the records and need a release from the student to access them.[41] Certain student information can be provided for directory purposes unless the student opts out.[42] Parents and eligible students have the right to review student records and to have incorrect or misleading

---

35 Pub. L. No. 104-191 (Aug. 21, 1996).

36 45 CFR 164.508.

37 45 CFR 164.524.

38 Acara v. Banks, 470 F.3d 569, 571 (5th Cir. 2006).

39 20 U.S.C. § 1232g.

40 20 U.S.C. § 1232g (b)(1).

41 20 U.S.C. § 1232g (d).

42 20 U.S.C. § 1232g (a)(5)(B).

information corrected.[43] FERPA does not create a private right of action which means private citizens cannot sue for damages under FERPA.[44]

### 6. PRIVACY ACT OF 1974

"The wrong which Congress hoped to right by the Privacy Act was the threat to an individual's right to privacy by the collection, maintenance, use and dissemination of personal information by the federal government."[45] The Privacy Act included the right to access and correct records[46] and required consent to release information about individuals from that individual.[47] Naturally, there are exceptions to this requirement to allow the government to do necessary work.[48] The Privacy Act was an important step forward, but it only addresses privacy as to information gathered by the federal government.

### 7. WIRETAP ACT

The Wiretap Act[49] provides limits to the interception, disclosure, or intentional use of "wire, oral, or electronic communication."[50] The Wiretap Act does provide for a private right of

[43] 20 U.S.C. § 1232g (a)(2).

[44] Gonzaga Univ. v. Doe, 536 U.S. 273, 287 (2002).

[45] Captain Robert E. Gregg, *The Privacy Act of 1974*, ARMY LAW., JULY 1975, at 25, 25–26.

[46] 5 U.S.C. § 552a(d).

[47] *5 U.S.C.* § 552a(b).

[48] *5 U.S.C.* § 552a(b)(1)-(11).

[49] Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) 18 U.S.C. §§ 2510-22, as amended by the Electronic Communications Privacy Act (ECPA).

[50] 164 A.L.R. Fed. 139 (Originally published in 2000).

action[51] as well as criminal penalties.[52] The Wiretap Act applies to "any person" committing a violation, so it is very broad in application.[53]

### 8. VIDEO PRIVACY PROTECTION ACT OF 1988

The Video Privacy Protection Act (VPPA) of 1988 prohibits the disclosure of what audio or visual recordings you may have watched.[54] The VPPA was passed as the result of a reporter finding out what videos Supreme Court nominee Robert Bork had been watching.[55] The VPPA provides for a private right of action for violations.[56]

### 9. STATE LAWS

#### a. SAMPLING OF STATE STATUTES

States have been very active in protecting the privacy of their residents. All fifty states now have breach notification laws.[57] Some states have enacted unique laws which may serve as a guide to determine what the future may hold for the law and what the states see as priorities for data privacy.

California recently passed a sweeping privacy act known as the California Consumer Privacy Act (CCPA). Key portions of the act include the right to access information collected

---

[51] 18 U.S.C. § 2520.

[52] 18 U.S.C. § 2511(4)(a).

[53] 18 U.S.C. § 2511(1).

[54] 18 U.S.C. § 2710.

[55] *See* S. Rep. No. 100-599, at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1 ("Senate Report"), *also available at* 1988 WL 243503. Cited by *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 278 (3d Cir. 2016).

[56] 18 U.S.C. § 2710(c).

[57] *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (September 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

about one's self, to find out what information has been sold or accessed, to opt out of the sale of information, and to request deletion of personal information.[58] It is set to go into enforcement as of January 1, 2020, but companies must "look back" one year.[59] If a company received a request on the first day the law is effective, they would need to look back into their records to January 1, 2019. Essentially, companies have to be able to track data sufficiently to adequately comply in 2020.

California is instructive for several reasons. Significantly, California's law was the product of a negotiation between an advocacy group which was on track to get enough signatures to get their version of an aggressive new data privacy law on the books through a referendum.[60] The legislative version passed at practically the last moment to avoid the referendum version from going on the ballot.[61] This tells us that people are interested in stronger data privacy than we have previously had. It also tells us that people's interest can be organized into political pressure. States with referendums may be subject to similar processes of citizen or advocacy group-driven laws. Any state, regardless of legislative process, may be subject to a concerted effort to pass new laws expanding privacy or perhaps efforts by large tech companies to pass laws to curtail a great expansion of consumer rights. Another concern with California is that it is one of the largest economies in the world.[62] Companies that want to do business there will have to comply with the

---

[58] Data protection principles—California Consumer Privacy Act—Consumer privacy rights, 1 Information Law § 8:82.54.

[59] Cal. Civ. Code § 1798.130(a)(2) (West).

[60] Lothar Determann, *New California Law Against Data Sharing*, 35 COMPUTER INTERNET LAW., Sept. 2018, at 1.

[61] *id*. (The legislature only debated the bill for six days).

[62] Associated Press, *California is now the world's fifth-largest economy, surpassing United Kingdom*, LA TIMES (May 04, 2018), https://www.latimes.com/business/la-fi-california-economy-gdp-20180504-story.html.

law by the year 2020. Thus, for companies with a national presence, California's law will become a de facto national law.[63] Finally, the application of the law in California may be closely watched by other states desiring to provide better privacy protection for their residents.

Illinois' Biometric Law is discussed under a later section. This law is another example of states taking the lead on privacy issues.

As of the date of this paper, Washington state is in the process of bringing forth a law called the Washington Privacy Act.[64] The current version distinguishes between data controllers and data processors similarly to the GDPR.[65] It has similar provisions to the CCPA, addresses specific de-identification and facial-recognition, but presently has no private right of action.[66]

Vermont's data broker law addressed the lack of regulation of those companies who buy and sell access to consumer data.[67] Data brokers listed as a result of the new law include Experian and Spokeo.[68] [69] The law requires data brokers to specify to consumers whether there is a

---

[63] Tony Romm, *Inside the lobbying war over California's landmark privacy law*, WASH. POST (February 9, 2019), https://www.mercurynews.com/2019/02/09/californias-landmark-privacy-law-sparks-lobbying-war-that-could-water-it-down/.

[64] Mitchell Noordyke, *The state Senate version of the Washington Privacy Act: A summary*, IAPP (March 26, 2019), https://iapp.org/news/a/the-state-senate-version-of-the-washington-privacy-act-a-summary/?mkt_tok=eyJpIjoiTjJRd01tWTBNall6TkdKaCIsInQiOiJDWklNWE9vbzJya2ZaTmJlQm1YQWUxNWJpWUNaTURHaE5CVGwxS1VZZld2TUhUQnduVEpvTDRMdWhvM2dXdEhnWnRCdko2YUE3NXVSRjg0MUR5djJSaWJjYmtPRFhCcGthUGE5XC9xV21uc1F0cFV0K1JlT2owXC9wYWswQTgzNlwvdSJ9.

[65] *id*.

[66] *id*.

[67] Steven Melendez, *A landmark Vermont law nudges over 120 data brokers out of the shadows*, FAST COMPANY (March 2, 2019), https://www.fastcompany.com/90302036/over-120-data-brokers-inch-out-of-the-shadows-under-landmark-vermont-law.

[68] *id*.

[69] Spokeo is a company which aggregates information to power their people search engine. The lawsuit against them by an individual who claimed they disseminated incorrect information about him set the standard for the level of harm that needs to be demonstrated for Article III standing in data breach cases. Spokeo, Inc. v. Robins, 136 S.Ct.1540 (2016).

mechanism to opt out of or restrict data collection.[70] It also requires disclosure of data breaches within the last year and mandates minimum security procedures.[71] However, it does not mandate an opt out procedure, right of access and review of data, information about how it was obtained, or a private right of action.[72]

### b. STATE COMMON LAW

Those harmed by data privacy breaches may be able to recover damages under common law claims such as negligence and invasion of privacy.

There are four types of invasion of privacy torts. Public disclosure of private facts is most common with data privacy breaches.[73]

The trouble with relying on common law claims is the multitude of lawsuits which may arise in a massive breach, the burden of proof on the claimants, and the fact that the harm has already been done. Once there is a public breach of data privacy, it cannot be undone. Further, there may be constitutional limitations on the use of common law privacy claims.[74] The focus should be on laws which provide guidance and incentives to protect people's personal information.

## 10. CONSTANT MAJOR BREACHES

It is impossible to avoid the conclusion that the protection of our privacy in the U.S. by organizations has failed. A brief summary of recent major breaches includes:

---

[70] Steven Melendez, *A landmark Vermont law nudges over 120 data brokers out of the shadows*, FAST COMPANY (March 2, 2019), https://www.fastcompany.com/90302036/over-120-data-brokers-inch-out-of-the-shadows-under-landmark-vermont-law.

[71] *id*.

[72] *id*.

[73] Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating A Common Law Approach for Data Breaches*, 127 YALE L.J. FORUM 614, 619 (2018).

[74] *id*. at 620.

As a credit bureau, Equifax stored sensitive information including social security numbers, birthdates, and, in some cases, credit card numbers, all of which were exposed in the breach.[75] The Equifax breach affected 143 million people.[76] Equifax is one of the three major credit reporting agencies in the U.S.[77] The breach can be attributed to the failure to timely install a patch on their system for a known cybersecurity vulnerability. However, the troubles for Equifax did not end there. There are additional concerns that executives sold stock between the time the breach was discovered and the time it was disclosed to the public.[78] Further, the delay from the discovery of the breach in July to its disclosure in September is concerning.[79] One might also question whether Equifax or the other credit bureaus should have access to people's private information without consumers directly consenting to have the credit bureaus collect, store, and share information. The Equifax breach shows the intersection between cybersecurity with the failure to install the patch, and privacy where millions of people's private data was exposed. It also raises issues of breach notification and officer and director liability.

The Target breach involved the exposure of personal data relating to 110 million consumers who were customers of the retailing giant.[80] The breach was due to a vulnerability with a vendor

[75] Sean L. Harrington, *Why the Equifax Breach Could be the Tipping Point*, 23 No. 16 WJSLR 2 (December 8, 2017).

[76] *id*.

[77] *id*.

[78] *id*.

[79] *id*.

[80] *In re Target Corp. Customer Data Sec. Breach Litig*., 64 F. Supp. 3d 1304 (D. Minn. 2014).

of Target's.[81] Clearly, effective management of third-party vendors is a key part of preventing a breach. It was alleged that Target did not live up to its own published policies.

Home Depot experienced a breach of credit card information on fifty-six million cards.[82] Similarly to Target, the vulnerability came about through a vendor.[83] While Target and Home Depot are examples of breaches due primarily to inadequate cybersecurity procedures and implementation, the next two have to do with policies regarding privacy.

Facebook is no stranger to controversy over its privacy policies and practices. However, the Cambridge Analytica scandal definitely stands out. Dr. Aleksandr Kogan used an application (app) to scrape information from the user's friends' information.[84] Facebook apparently allowed these types of activities for researchers, but researchers were not supposed to transfer the data for any monetary benefit such as advertising.[85] However, Dr. Kogan did provide the information to Cambridge Analytica which used it as part of Donald Trump's presidential campaign.[86] Of the fifty million files transferred to Cambridge Analytica, only 270,000 users actually consented to their information being used for research.[87] Questions have been raised about Facebook's

---

81 Michael Kassner, *Anatomy of the Target data breach: Missed opportunities and lessons learned*, ZDNET (February 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

82 Tara Seals, *Home Depot to Pay $27.25m in Latest Data Breach Settlement*, INFOSECURITY MAGAZINE (March 13, 2017), https://www.infosecurity-magazine.com/news/home-depot-to-pay-2725m/.

83 *id.*

84 Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*. N.Y. TIMES (March 19, 2018), https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

85 *id.*

86 *id.*

87 *id.*

disclosure as to the gathering of the information.[88] Google's Google Plus suffered an exposure of fifty-two million users' information due to a bug in the system.[89] This followed a breach involving 500,000 users' private data which Google did not disclose until the New York Times reported on it.[90] More recently, Google failed to disclose a microphone which was included in the design of its "Nest Secure," which is a home security system.[91] While we do not know if this resulted in the exposure of anyone's private information, clearly a listening device designed to be placed in one's home raises privacy concerns and not disclosing it fuels the distrust of the public and their representatives in government.

These are only a sample of major breaches. A national survey of security professionals funded by Egress reported that eighty-three percent of U.S. organizations have accidentally breached sensitive data.[92]

### 11. COST & DIFFICULTY IN COMPLYING WITH CURRENT LAWS

The problem with the current regulatory scheme is that companies with a national presence must comply with laws in all fifty states. Some of these laws are new and untested. This means not only having to navigate many different requirements, it means that laws may have technical errors or ambiguities in them. Divining the meaning of a statute or regulation is time consuming

---

88 *id*.

89 Craig Johnson, *What the latest Google data breach means for you*, CLARK (December 11th, 2018), https://clark.com/technology/what-the-latest-google-data-breach-means-for-you/.

90 *id*.

91 Arjun Panchadar & Akanksha Rana, *Google fails to disclose microphone in Nest Secure*, REUTERS (February 20, 2019), https://www.reuters.com/article/us-alphabet-nest/google-fails-to-disclose-microphone-in-nest-secure-idUSKCN1Q92F8.

92 MTS Staff Writer, *Survey: 83 Percent of US Organizations Have Accidentally Exposed Sensitive Data*, MARTECHSERIES (February 25, 2019), https://martechseries.com/analytics/data-management-platforms/privacy-and-regulations/survey-83-percent-u-s-organizations-accidentally-exposed-sensitive-data/.

and one is still in some respects guessing as to how an agency or court will interpret it. To be fair, companies certainly are capable of doing this, but for laws with a national implication, this seems like an unnecessary drain on resources. Privacy advocates will argue that some states provide greater protections and it is likely true that some states will provide greater protection than an eventual federal law, but there are two concerns with the status quo. One, that breaches are happening despite tough laws in some states. And two, that tough laws may go too far and actually prevent positive opportunities for innovation.

### 12. COMPLEX REGULATORY SCHEME PROMOTES A CULTURE OF COMPLIANCE

As noted above, breaches keep occurring despite the current patchwork of state and federal laws. It is possible that the extensive number of laws which a company must comply with actually helps perpetuate a culture of compliance rather than privacy protection. A clearer roadmap to a successful data privacy and security program may actually get the results people are hoping for. With fewer conflicting expectations and, perhaps, clearer consequences for failing to live up to those expectations, the focus can be more on proactively preventing breaches or abuses of privacy.

### 13. THE U.S. PUBLIC IS CONCERNED ABOUT PRIVACY

According to research by the Pew Research Center, "[s]ome 68% of internet users believe current laws are not good enough in protecting people's privacy online."[93] Interestingly, one research study found that Americans were more concerned about privacy than job creation.[94]

---

[93] *The state of privacy in post-Snowden America*, PEW RESEARCH (September 21, 2016), https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

[94] Dawin Brown, *Americans are more concerned with data privacy than job creation, study shows*, USA TODAY (November 9, 2018), https://www.usatoday.com/story/money/2018/11/09/americans-more-concerned-data-privacy-than-healthcare-study-says/1904796002/.

Software analytics company SAS did a survey where they found 73% of respondents are more concerned about their privacy than they were a few years ago.[95]

### 14. CACOPHONY OF VOICES ARE PUSHING FOR A NATIONAL LAW

The intensity of interest and activity around the possibility of a comprehensive federal law is so great that the International Association of Privacy Professionals (IAPP) has created a members-only Privacy Watch tool for members to keep track of developments.[96]

"Big Tech" companies such as Google and Facebook are pushing for a national law; as are industry groups, politicians, academics, and privacy advocacy groups. The landslide of people and groups asking for a national law can be confusing and overwhelming. However, I believe that it means that the will to pass a law exists and the battle is along the lines of what it will contain rather than should we have one.

In testimony before the House Consumer Protection and Commerce Subcommittee, Brandi Collins-Dexter, Senior Campaign Director of the Color of Change, an online civil rights organization stated: "If we fail in the mission to ensure our rights online are protected, we stand to render many of our offline rights meaningless."[97]

---

[95] Taylor Armerding, *National Data Privacy Day is Wishful Thinking*, FORBES (January 23, 2019), https://www.forbes.com/sites/taylorarmerding/2019/01/23/national-data-privacy-day-is-wishful-thinking/#75d7c7e61128.

[96] *US Federal Privacy Watch*, IAPP (last visited March 3, 2019), https://iapp.org/resources/topics/us-federal-privacy-watch/.

[97] Jessica Davis, *Congress Weighs National Data Privacy Law to Reduce Data Risk*, HEALTH IT SECURITY (February 27, 2019), https://healthitsecurity.com/news/congress-weighs-national-data-privacy-law-to-reduce-data-risk.

Jan Schakowsky, D-IL., who is the head of the Consumer Protection and Commerce Subcommittee stated: "We have seen time and again that self-regulation is not protecting consumers."[98]

Senator Marco Rubio proposes using the Privacy Act of 1974, which was discussed above, to address privacy concerns. He argues that a patchwork of state laws is ineffective, and that the Internet is interstate commerce and therefore within Congress's purview to regulate.[99]

The American Banking Association (ABA) has also called for "uniform national privacy standards."[100] The ABA argues that not having a uniform standard makes it hard for consumers to understand their rights.[101] The ABA advocated for the Gramm-Leach-Blilely Act to be a model for the federal standards.[102] Given the GLBA regulates banks, this would certainly simplify implementation of a national data privacy law for financial institutions such as banks.[103]

The Government Accountability Office (GAO) has come out in favor of a comprehensive federal privacy law pointing to the Cambridge Analytica and Facebook scandal and the E.U.'s General Data Protection Regulation (GDPR) which became effective in May 2018.[104]

---

98 Stephanie Condon, *Congress considers a national standard for data privacy*, ZDNET (February 26, 2019), https://www.zdnet.com/article/congress-considers-a-national-standard-for-data-privacy/.

99 Marco Rubio, *Congress needs to address consumer data privacy in a responsible and modern manner*, THE HILL (January 16,2019), https://thehill.com/blogs/congress-blog/technology/425557-congress-needs-to-address-consumer-data-privacy-in-a.

100 *ABA Calls for Uniform National Privacy Standards*, ABA JOURNAL (February 26, 2019), https://bankingjournal.aba.com/2019/02/aba-calls-for-uniform-national-privacy-standards/.

101 *id*.

102 *id*.

103 *id*.

104 Jack Corrigan, *Researchers recommended lawmakers give regulators more power to write rules and punish the companies that break them*, NEXTGOV (February 13, 2019), https://www.nextgov.com/policy/2019/02/gao-urges-congress-start-moving-privacy-law/154875/.

While there are too many federal privacy law proposals to set forth here, some examples are provided:[105] CDT - Center for Democracy & Technology has proposed baseline federal legislation that sets reasonable limits on the use, collection, and sharing of personal information and provides individual rights to access, correct, delete, and port data.[106]

Representative Suzan DelBene introduced the ‘‘Information Transparency & Personal Data Control Act,’’ which would establish an "opt-in" framework for companies that collect sensitive personal information and require them to present privacy policies in "clear and plain language."[107]

Senator Ron Wyden introduced the Consumer Data Protection Act, which proposes more power and staff for the FTC, transparency about how corporations share, sell and use data; and creates penalties and jail time for executives.

Senator Marco Rubio proposed the American Data Dissemination (ADD) Act which would expand the Privacy Act of 1974.[108] The FTC would recommend regulations to Congress and if Congress does not act, then the FTC would pass a final rule.[109] The law requires regulations be

---

[105] For a comprehensive discussion of proposals, *see*: Müge Fazlioglu, *Consensus and Controversy in the Debate Over US Federal Data Privacy Legislation*, IAPP (January 15, 2019), https://iapp.org/news/a/new-iapp-guide-to-u-s-privacy-law-proposals/.

[106] *Americans Deserve a Law Protecting Their Digital Privacy — Here's Our Proposal,* CDT (December 13, 2018), https://cdt.org/press/americans-deserve-a-law-protecting-their-digital-privacy-heres-our-proposal/.

[107] *DelBene Introduces Legislation to Regulate Consumer Privacy,* U.S. CONGRESSWOMAN SUZAN DELBENE (September 20, 2018), https://delbene.house.gov/news/documentsingle.aspx?DocumentID=2395.

[108] Marco Rubio, *Congress needs to address consumer data privacy in a responsible and modern manner,* THE HILL (January 16,2019), https://thehill.com/blogs/congress-blog/technology/425557-congress-needs-to-address-consumer-data-privacy-in-a.

[109] *id*.

scaled to allow small and new organizations to be able to comply.[110] The law would preempt state laws.[111]

Senators Klobuchar and John Kennedy released a draft law which gives consumers the right to opt-out and keep their information private by disabling data tracking and collection, and greater transparency. It requires breach notification in seventy-two hours and companies must have a privacy program.

### 15. INTERNATIONAL COMPETITIVENESS

In many matters, the U.S. is looked upon as a leader in the world. However, at the moment, the E.U. is leading the charge as to data privacy laws.[112] It would help shore up the U.S.'s position as an economic and moral leader to pass stronger and effective data privacy laws. Further, given the U.S.'s influence, a comprehensive national law could steer the international laws in a direction more desirable to U.S. interests.[113]

While international companies are certainly accustomed to the challenges of differing laws and cultures, conflicting requirements can cause difficulties for a company in situations where more than one nation's laws are implicated. For example, if the E.U. requires a notification in forty-five days and a U.S. jurisdiction requires one in ninety days, there is a potential for conflict between regional management. The quality and quantity of information available to give in forty-

---

110 *id.*

111 Malcolm Owen, *American Data Dissemination Act seeks to legislate how the tech industry uses your data*, APPLE INSIDER (January 16, 2019), https://appleinsider.com/articles/19/01/16/american-data-dissemination-act-seeks-to-legislate-how-the-tech-industry-uses-your-data.

112 Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html.

113 *IA Privacy Principles for a Modern National Regulatory Framework*, INTERNET ASSOCIATION, https://internetassociation.org/wp-content/uploads/2018/09/IA_Privacy-Principles-For-A-Modern-National-Regulatory-Framework_full-doc.pdf (last visited May 18, 2019) (argues that establishing a federal data privacy law would reinforce the U.S. leadership position).

five days differs from the same in ninety days. A jurisdiction's media and public will judge information based on local practice. An E.U. manager may push for earlier disclosure where someone accustomed to a longer lead time may be uncomfortable with an earlier disclosure. This can be abated if as many nations as possible pick the same time frame so jurisdictions have a more uniform expectation of how much information can be realistically gathered for that initial notice.

With the GDPR in the E.U., and the E.U.'s adequacy ruling on Japan's law, the U.S. is at risk for being left behind on data portability. The U.S. currently relies on a privacy shield negotiated with the E.U. after the Safe Harbor agreement was set aside.[114] The privacy shield is not an adequate long-term solution as it is subject to lawsuits and enforcement issues. It would be a better solution to have a set of U.S. laws that the E.U. would be willing to find adequacy with to keep markets more open to U.S. companies.

## III. CHALLENGES TO CREATING A NATIONAL PRIVACY LAW

### A. THE COMMODITIZATION OF PERSONAL INFORMATION

Personal information, when gathered in large quantities, is so valuable that it has been dubbed the "new oil."[115] The U.S. is home to technology giants like Google, Twitter, and Facebook. In the absence of strong privacy regulation, these companies built their fortunes in large part based on using the analysis of private information to market goods and services to consumers. In exchange, consumers get "free" access to their platforms. Proponents will point to

---

[114] *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, EUROPEAN COMMISSION (February 2, 2016), http://europa.eu/rapid/press-release_IP-16-216_en.htm.

[115] Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, ABA BLT (September 19, 2018), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus/.

the growth and innovation of the industry. Detractors will point to the deceptive and opaque practices which seem common where consumers are not aware of the depth of information that is being gathered, analyzed, and sold.

An argument can be made that our current situation is untenable and that people's rights to privacy are not being protected. Therefore, even though changing the law means changing business models, this is not a negative outcome. Further, there is evidence that new models can be successful. The New York Times continues to do business successfully in the E.U., post-GDPR.[116] Despite eliminating behavior-based advertising and open exchange advertisement buying in Europe, the news outlet continues to see growth in advertising revenue.[117] The key seems to be finding alternate ways to fund through advertising if the study concluding that Americans will not pay for privacy is correct. According to the Center for Data Innovation study, while Americans want less data to be collected about them, only 26.7% are willing to pay subscription fees to protect their private data while using sites like Google and Facebook.[118]

The question is finding a balance between stringent privacy regulations which may arguably stifle innovation and end, in part, the number of free services available and the status quo. The status quo includes the Cambridge Analytical scandal and Google tracking people's locations even after it claimed it stopped.

---

[116] Jessica Davies, *After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue*, DIGIDAY (January 16, 2019), https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/.

[117] *id.*

[118] Nicole Lindsey, *New Study Shows that Americans will not Pay for Online Privacy*, CPO MAGAZINE (February 1, 2019), https://www.cpomagazine.com/data-privacy/new-study-shows-that-americans-will-not-pay-for-online-privacy/.

### B. RIGHTS RESERVED TO STATES

Under the Tenth Amendment, all rights not expressly given to the federal government are reserved to the states.[119] Thus, states can regulate privacy because it is not expressly given to the federal government to regulate. However, this can be overcome by the Interstate Commerce Clause which allows the federal government to regulate commerce among the states.[120] Further, the application of the Supremacy Clause would allow for preemption of state law. Also, state law which so impedes commerce among the states may be unconstitutional under the Dormant Commerce Clause.[121]

### C. WILL BIG TECH SUPPORT A FEDERAL LAW WITHOUT PREEMPTION?

It seems unlikely that so called big tech would support a federal law without preemption due to the complications of complying with fifty-one different laws. However, big tech could still potentially benefit from a federal law that achieved adequacy with E.U. law and caught the U.S. up with the many other nations which have been instituting stronger privacy laws on a national level. Big tech would benefit from improved portability of information. Also, big tech would already have experience in complying with the GDPR and it's unlikely that any U.S. law would be more stringent. The question is not whether there will be preemption; rather, how much of state law would need to be preempted to satisfy big tech and other commercial interests without losing support needed from state governments and privacy advocacy groups?

---

[119] U.S. CONST. amend. X (Text *supra*).

[120] U.S. CONST., Art. I, § 8, cl. 3 (Text *supra*).

[121] Tony Glosson, *Data Privacy in Our Federalist System: Toward an Evaluative Framework for State Privacy Laws*, 67 FED. COMM. L.J. 409, 415 (2015).

While members of both parties have expressed support for a comprehensive federal privacy law, they differ on preemption.[122] Republicans favor preemption to avoid the cost of complying with a patchwork of laws.[123] Democrats worry that a federal law may be weaker than the existing state laws protecting consumer privacy, so preemption would reduce consumer protection in that instance.[124] However, Republican Roger Wicker argued the data privacy framework should not mean one that is weaker than what the states are developing.[125]

Privacy is certainly not the only area of the law to deal with fifty states of laws. Professor Woodrow Hartzog testified before the Senate Commerce, Science and Transportation Committee hearing that he teaches his students to deal with a fifty-state patchwork.[126]

### D. RESISTANCE TO ADOPTING E.U. LAW

Some Americans may resist anything related to Europeans. However, it is important to focus on the benefits of improved and consistent law, particularly in the area of continued prosperity for Americans. It is unimportant that we adopt laws that may have European roots; rather, we should focus on what the laws can do for us. Or, if the carrot doesn't work, the stick will be what will happen to the U.S. if we don't have a cohesive set of privacy laws that are sufficiently on par with other large economies with which we want to do business.

---

122 Cozen O'Connor, *Congress Holds Hearings on Privacy and Data Protection*, CYBERLAW MONITOR (March 6, 2019), http://cyberlawmonitor.com/2019/03/05/congress-holds-hearings-on-privacy-and-data-protection/.

123 *id.*

124 *id.*

125 *id.*

126 Henry Kenyon, *Federal Regulation on Privacy Must Trump State Laws Senate Panel Told,* CQ ROLL CALL WASHINGTON DATA PRIVACY BRIEFING (Congressional Quarterly Inc., 2019).

Cisco chief legal and compliance officer Mark Chandler was quoted in the *Financial Times*: "We believe that the GDPR has worked well and that with a few differences, that is what should be brought in in the U.S. as well."[127]

### E. MAJOR ECONOMIC POWERS NOT SIGNING ON TO E.U. STANDARDS

One potential impediment to the U.S. adopting standards similar to the E.U. is that major economic powers of China and Russia are unlikely to adopt the standards in earnest. The argument that the U.S. must be in parity with the E.U. is undermined if China and Russia don't adopt similar standards. Countries will need to find ways if they want those markets, so the U.S. may take the point of view that they can demand the same accommodations.

### F. GDPR IS UNTESTED

A challenge to adopting a regulatory framework based on the GDPR is that the GDPR just moved into effect on May 25, 2018. As a result of its recency, any new or enhanced aspects of the GDPR are largely untested. The U.S. will not want to blindly adopt laws for which the E.U. may have "buyer's remorse." The U.S. will want to be careful to avoid adopting any undesired unintended consequences of certain aspects of the GDPR.

A goal of a comprehensive law would be to clear up as many conflicting and potentially overburdensome requirements as possible created by both new and existing laws to achieve the desired outcome of protecting the public's private data.[128] A risk with proceeding to make changes of course is that people will not want ambiguities resolved in a fashion which they perceive limits their rights as either consumers or businesses.

---

[127] Alana Foster, *Tech giants urge US to adopt GDPR law*s, IBC365 (February 5, 2019), https://www.ibc.org/regulation/tech-giants-urge-us-to-adopt-gdpr-laws/3570.article (quoting the Financial Times).

[128] Lothar Determann, *New California Law Against Data Sharing*, 35 COMPUTER INTERNET LAW., Sept. 2018, at 1.

One of the concerns expressed about the GDPR and CCPA are the ambiguities in the current laws. Certainly, one would not want to adopt the law wholesale without trying to iron out any unintended ambiguities or unintended consequences.

### G. RISK OF STIFLING INNOVATION

Companies such as Google and Facebook experienced rapid growth in part due to not charging for access in exchange for information about users.[129] Future regulations which are too strict can arguably stifle innovation. While Google and Facebook have the deep pockets to adapt to a changed regulatory structure and continue, one might argue that the bar to entry can be made too high if the regulatory structure is too strict and thus expensive and restrictive. According to Denise Zheng of Business Roundtable, the current state measures are barriers to innovation which businesses would find unworkable.[130]

A counterargument is that a new law can eliminate some activities that simply should not be allowed. For example, cellular carriers selling people's geolocation information without their knowledge or consent.[131]

Rather than stifling business growth, it may be argued that effective privacy laws which are embraced by organizations can help businesses grow. The Capgemini study which interviewed 6,000 individuals and 1,000 industry executives in eight countries found that consumers were

---

[129] *id*. at 9.

[130] Emily Birnbaum & Harper Neidig, *State Rules Complicate Push for Federal Data Privacy Law*, THE HILL (March 5, 2019), https://thehill.com/policy/technology/432564-state-rules-complicate-push-for-federal-data-privacy-law.

[131] Joseph Cox, *I Gave a Bounty Hunter $300. Then He Located Our Phone*, MOTHERBOARD (January 8, 2019), https://motherboard.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.

likely to spend more money, time, and interact more frequently with organizations they believed would protect their private data.[132]

### H. POLITICS AS USUAL

For a large portion of the time this paper was being written, the government was shut down.[133] Few people would argue that a government shutdown for any length of time is in the best interests of the economy, but it still happened. Unfortunately, despite a strong desire to address issues of data privacy and security, it's unclear that our representatives in government will have the drive to negotiate a new law.

Past attempts to pass federal privacy laws have stalled out in committee. One reason is because of disputes over committee jurisdiction.[134] Certainly members of Congress have different priorities from each other and different philosophies.

## IV. POSSIBLE PATHS FORWARD TO A NATIONAL PRIVACY LAW

This section will explore the process to arrive at consensus, possible vehicles for a comprehensive privacy law, and an analysis of major provisions which may be included in such a law.

---

[132] *GDPR is good for business says Capgemini study*, MONEY DONUT (May 21, 2018) https://money.taxdonut.co.uk/news/gdpr-good-business-says-capgemini-study.

[133] Michael Collins, et. al., *Trump signs measure to temporarily reopen government, setting up new battle over border wall*, USA TODAY (January 25, 2019), https://www.usatoday.com/story/news/politics/2019/01/25/shutdown-senate-leaders-talk-flight-delays-reported-airports/2676022002/.

[134] Daniel R. Stoller, *2019 Outlook Data Privacy Bill*, BLOOMBERG (December 28, 2018), https://news.bloomberglaw.com/privacy-and-data-security/2019-outlook-data-privacy-bill-to-move-amid-corporate-push.

### A. PROCESS FOR CONSENSUS

One of the challenges of having a groundswell of support for a federal privacy law but no clear agreement on what it should contain is how to come to consensus and get a bill passed. This section discusses the various avenues for dialogue about the prospect of a comprehensive federal privacy law.

#### 1. INTEL'S PROPOSAL: THE INNOVATIVE & ETHICAL DATA USE ACT

Intel, one of the "Big Tech" companies, has put forth its own draft bill called the Innovative and Ethical Data Use Act and invited comments from privacy experts.[135] The public may also comment.[136] This collaborative approach gives hope that there are parties sincerely interested in moving the law forward. One might be cynical and say that by drafting a bill and hosting the discussion, that Intel is trying to steer the direction of the debate. This is not surprising or truly a concern as several groups have staked out positions and will try to steer the discussion in a way which benefits their point of view. One of the main components of Intel's proposal is federal preemption of state law.

#### 2. CONGRESSIONAL HEARINGS

Congress has been very active recently with holding hearings on privacy-related issues.[137] Televised hearings can serve to raise public awareness of the issue of privacy and the nuances of a comprehensive privacy law.

---

[135] Ryan Chiavetta, *Intel launches online portal for consultation on its draft US federal privacy law*, IAPP (Nov 8, 2018), https://iapp.org/news/a/intel-launches-online-portal-for-consultation-on-its-u-s-federal-privacy-law/.

[136] *id.*

[137] Recent hearing include: GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation by the U.S. Senate Committee on the Judiciary retrieved March 14, 219 from https://www.judiciary.senate.gov/hearings/watch?hearingid=18A4900C-5056-A066-603B-49825BF70512. The Senate Committee on Commerce, Science, and Transportation held a hearing on February 27, 2019 entitled "Policy Principles for a Federal Data Privacy Framework in the United States" retrieved March 14, 2019 from https://www.commerce.senate.gov/public/index.cfm/hearings?ID=CBA2CD07-4CC7-4474-8B6E-513FED77073D.

## B. ANALYSIS OF MAJOR PROVISIONS & RECOMMENDATIONS

### 1. DELAYED IMPLEMENTATION

One potential way forward is to pass a comprehensive law but allow sufficient time to implement it. It seems like the practice is to give about two years to implement, but this seems problematic from the standpoint that it doesn't give much time to produce regulations and guidance. In the case of the GDPR, several E.U. members had not passed their required national laws by the implementation date of the GDPR.[138] In the case of the California Consumer Privacy Act (CCPA), the California Attorney General is still having open meetings about the law less than a year before the law will be enforced and has not yet produced regulations to implement the law.[139]

### 2. RIGHT TO PRIVACY AS A FUNDAMENTAL RIGHT

The European Union's Charter of Fundamental Rights recognizes privacy as a fundamental right.[140] The concept of privacy as a fundamental right has support within the U.S. from such organizations as the Center for Democracy and Technology (CDT).[141]

What are the implications of making privacy a fundamental right? It would pave the way for legislation and reduce the chances of successful legal challenges to data privacy legislation.

---

[138] *EU Member State GDPR Implementation Laws and Drafts*, IAPP: RESOURCE CENTER, https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/ (last visited May 19, 2019).

[139] *California Consumer Privacy Act (CCPA)*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE: OFFICE OF THE ATTORNEY GENERAL, https://www.oag.ca.gov/privacy/ccpa (last visited April 1, 2019).

[140] U.N. Charter art. 8 states: "1. Everyone has the right to the protection of personal data concerning him or her. 2. 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. 3. Compliance with these rules shall be subject to control by an independent authority."

[141] *Americans Deserve a Law Protecting Their Digital Privacy — Here's Our Proposal*, CDT (December 13, 2018), https://cdt.org/press/americans-deserve-a-law-protecting-their-digital-privacy-heres-our-proposal/.

One area of potential confusion with making privacy a fundamental right is that typically constitutional rights in the U.S. are focused on rights to safeguard against government intrusions. However, when we think of major breaches of data security or privacy, many are by private companies. The E.U. right to data privacy is not limited to governmental intrusion and thus would be a change in perspective of fundamental rights in the U.S. In order to create a fundamental right to data privacy, we would need to amend the U.S. Constitution as discussed in the next section.

### 3. CONSTITUTIONAL AMENDMENT WITH RIGHT OF PRIVACY

Perhaps a good first step in the direction of a comprehensive federal law would be to amend the U.S. Constitution to explicitly guarantee the right to privacy. As it stands, there are Amendments which address particular rights which relate to privacy and there are Supreme Court cases which find the right to privacy exists within the penumbra of the rights guaranteed by the Constitution.[142] Eleven states have guaranteed the right to privacy in their Constitutions.[143] A constitutional Amendment explicitly guaranteeing the right to privacy would give more power to privacy legislation and give great impetus to move forward with a comprehensive structure. Unfortunately, a constitutional Amendment is a time consuming and lengthy process which is certainly far from guaranteed to succeed.[144]

### 4. CHANGES TO FTC AUTHORITY & FUNDING

Assuming the FTC will continue to take the lead at the federal level on consumer privacy, then they will need additional funding and staff as they take on additional responsibility. Given

---

[142] Lee Goldman, *The Constitutional Right to Privacy*, 84 DENV. U. L. REV. 601 (2006).

[143] California has a right to privacy and New Hampshire recently added one. *See*, NCSL, *Privacy Protections in State Constitutions*, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

[144] *Constitutional Amendment Process*, NATIONAL ARCHIVES (last viewed March 28, 2019), https://www.archives.gov/federal-register/constitution.

that data breaches are announced almost daily, even if the FTC only went after the highest profile cases, they may be hard pressed to keep up. The Consumer Data Protection Act (CDPA) proposes additional staff for the FTC.[145]

Further, the practice of obtaining an order against an organization with serious deficiencies in protection of privacy is an insufficient deterrent.[146] The FTC needs the ability to levy serious consequences for serious violations the first time around.

Even with additional funding and additional staff, it seems unwise to exclude state attorneys general (AGs) from enforcement. The AGs have been leading the charge, and regardless of any change of the law, it would be wise to allow them to continue to enforce the law on the behalf of their residents.

### 5. ENFORCEMENT

#### a. CRIMINAL PENALTIES FOR EXECUTIVES

The CDPA proposed by U.S. Senator Ron Wyden of Oregon would add fines and even incarceration for company executives who misuse Americans' private information.[147] While a dramatic step, it seems likely that executives would be more likely to fear financial consequences and fallout from their boards and institutional investors. Likely only the very worst of cases would be prosecuted meaning much more attention needs to go to available civil remedies which are also substantial in the CDPA.

---

145 Security Experts, *New Federal Consumer Data Protection Act Proposed On Thursday*, ISBUZZNEWS (November 2, 2018), https://www.informationsecuritybuzz.com/expert-comments/new-federal-consumer-data-protection-act-proposed-on-thursday/.

146 Michael Scully & Cobun Keegan, *IAPP Guide to FTC Privacy Enforcement*, IAPP (2017), https://iapp.org/media/pdf/resource_center/Scully-FTC-Remedies2017.pdf.

147 Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy, Ron Wyden U.S. Senator for Oregon (November 1, 2018), https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

### b. CIVIL PENALTIES

Penalties need to be sufficient to deter poor data privacy practices even for the largest companies. One way to achieve this is to make fines payable up to a percentage of the company's revenue.

### c. ENFORCEMENT RESPONSIBILITY

While it is not a foregone conclusion, it seems logical to place enforcement responsibility for a comprehensive federal data privacy law with the FTC due to their long experience bringing enforcement actions in this arena.

### d. PRIVATE RIGHT OF ACTION

As discussed above, many laws relevant to data privacy have private right of action, meaning individuals can sue violators on their own behalf. Other laws do not. The potential problem with a private right of action is the threat of nuisance suits. The threat of a suit might allow a complainant to extract a settlement. If this were the case, the law may not be having the intended effect of improving data privacy. The advantage of a private right of action is that if the government fails to intervene, an individual can assert their rights. The risk of frivolous suits can be overcome with sufficient safeguards and dispute resolution mechanisms. To not have an option for a private right of action leaves individuals at the mercy of politics and limited budgets for prosecuting claims.

### e. SCOPE

It is important to determine who the law will be enforced against. In this respect, it would be helpful to limit the scope of the law to data privacy to make it more realistic to define against whom it could be enforced. It will be important to consider what size business or organization can realistically comply with whatever law is eventually passed. On a related note, the law could be

scaled to allow flexibility for smaller entities to manage data privacy without the law being an insurmountable barrier to entry.

### 6. FEDERAL MINIMUM WITH ALLOWED STATE ENFORCEMENT OF STRICTER STANDARDS

One potential way to lessen the impact of state misgivings about a federal "takeover" of data privacy law is to make sure that states continue to have the ability to enforce data privacy law, including federal law. Thus, if the concern is that a particular administration is not "tough" enough for a state, that state's attorney general could pursue enforcement actions on behalf of their state residents.

### 7. GEOLOCATION

Geolocation is just what it sounds like. It is the ability to track you by location. Sometimes it can be very specific. This can be used to find your lost phone, track a child or spouse, limit what you can see on the Internet based on your location, provide accurate driving directions, and push advertising to you based on your location. The concern is that without strong legislation, geolocation can be abused for surveillance and intrusive advertising.

### 8. ARTIFICIAL INTELLIGENCE

Artificial intelligence is a machine replacing the thinking of a human, but at a faster or more accurate rate. Artificial intelligence has great promise in many areas to reduce the cost of services and improve the accuracy of services. In the area of diagnosing skin cancer, for example, artificial intelligence has been trained to accurately identify types of tumors and can even do so more accurately than humans.[148] There are two challenges for privacy here right away. One is that someone must have access to the massive amounts of data they are feeding the program in the

[148] Agence France Presse, *Computer learns to detect skin cancer more accurately than doctors*, THE GUARDIAN (May 28, 2018), https://www.theguardian.com/society/2018/may/29/skin-cancer-computer-learns-to-detect-skin-cancer-more-accurately-than-a-doctor.

first place. Was this data obtained with consent? Was the consent obtained with a disclosure that the data would be used for artificial intelligence? Second, there is a concern that artificial intelligence can be used to invade people's privacy by scanning their faces or their gait as they walk through public places. It may take data available from numerous sources to ascertain private and personal information about you in ways previously not possible. Artificial intelligence could be used to determine if someone is likely pregnant or getting a divorce, for example. The GDPR has a requirement there be sufficient disclosure of any automated decision-making processes.[149]

### 9. BIOMETRICS

As defined by the Illinois Biometric Information Privacy Act, biometric identifiers consist of "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[150] Any definition in the law needs to be sufficiently broad to encompass emerging or unanticipated biometrics. There is a great risk of false positives and potential for racial profiling when using technologies like facial recognition in law enforcement.[151] Likewise, the use of facial recognition famously identified a number of members of the U.S. Congress as criminals.[152]

---

[149] *GDPR*, *supra* note 3, at art. 22.

[150] 740 Ill. Comp. Stat. Ann. 14/10 (The statute contains a lengthy paragraph on what is not biometric identifiers). "'Biometric information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers."

[151] Jeffrey Dastin, *Amazon's face ID tool mismatched 28 members of Congress to mugshots: ACLU*, BUSINESS INSIDER (July 26, 2018), https://static1.businessinsider.com/r-amazons-face-id-tool-mismatched-28-members-of-congress-to-mugshots-aclu-2018-7.

[152] *id*.

### 10. RIGHT TO ACCESS & CORRECT

The right to access your records is essential so that you know what is being collected about you and whether it is accurate or not. This right already appears in several laws such as the GDPR and FERPA.

Closely related to the right to access is the right to correct your records. This right explicitly exists in the GDPR and FERPA. With reasonable exceptions, this should be a right under federal law. In a consumer setting, it would be to the advantage of the merchant to have accurate information in any event.

### 11. RIGHT TO BE FORGOTTEN

The E.U. has the so-called "right to be forgotten."[153] The idea is that you can request that your information be removed from a database.[154] While it is a powerful right, it certainly must be limited to allow organizations to meet their legal obligations. An organization may need to retain your information based on the need to process your order, to demonstrate compliance with the law, in anticipation of litigation, and so on. Even with those limitations it is a great tool for data minimization. Consumers can opt to limit the personal data they disclose and thus reduce the chance of identity theft and other unwanted intrusions.

### 12. CONSENT

Consent under U.S. law defaults to "opt out."[155] This means that in most circumstances, you will be included in databases and marketed to. If you do not want your information shared, you need to notify the organization in the manner proscribed in their privacy notice.

---

153 *GDPR, supra* note 3, at art. 17.

154 *Id.*

155 Anita L. Allen, *Privacy Law: Positive Theory and Normative Practice*, 126 HARV. L. REV. F. 241, 249 (2013).

Consent in the E.U. runs on "opt in," which means you have to affirmatively agree to your information being shared.[156]

The U.S. should adopt "opt in" and GDPR quality notices which are transparent and understandable.[157] Consumers will benefit from improved privacy and merchants will benefit from marketing more accurately to people who purposefully provided their information.

### 13. PREEMPTION

Federal preemption has been left for last in this section due to the fact that it seems premature to discuss federal law displacing state law before people have agreed on what the essential features of a federal law would be. Due to the myriad of state laws which are used to address privacy even if they do not necessarily explicitly name privacy, it will be unrealistic to preempt all state laws relevant to data privacy law. Generally speaking, industry favors preemption and privacy advocates do not.[158]

The GLBA and HIPAA do not preempt state laws.[159] Some states have passed laws tougher than the federal minimums set forth in these laws.[160] Updates to the Fair Credit Reporting Act (FCRA), however, do have preemption.[161] It is important to note that consumers did get better protections in exchange for the preemption of state laws.[162] This is important to note for a strategy

---

156 *id*.

157 *Writing a GDPR-compliant privacy notice (template included)*, GDPR-EU, https://gdpr.eu/privacy-notice/ (last visited April 1, 2019).

158 Peter Swire, *US federal privacy preemption part 1: History of federal preemption of stricter state laws*, IAPP (January 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/.

159 *id*.

160 *id*.

161 *id*.

162 *id*.

going forward on preemption. Any adoption of preemption needs to be a part of a package that can be clearly communicated to the public as in improvement in their rights. This also points to why it is important to table discussions of preemption until there is a clear understanding of what one gets in exchange for preemption.

## V. OVERALL RECOMMENDATIONS & CONCLUSION

One important corner for all of the stakeholders to turn is an attachment to how privacy is currently handled in their state or industry. One example to look at is the length of time to report a breach. If one jurisdiction has a forty-five-day window and another has thirty, it's unlikely that we can conclusively prove one is the best and fairest. An earlier or later report will have an impact on the immediate quality of the disclosure. If we have the same time, we can have similar expectations. Let us have a consistent measure and, even better, have the same one as our E.U. trading partners. Likewise, we should adopt the same language whenever possible. For example, the concept of data controller and data processor under the GDPR. These make useful distinctions as to the level of responsibility for safeguarding personal data. There is no need to reinvent concepts and terminology. Further, whenever we can logically use common language and rules, we can share in the development of the law through cases and enforcement actions leading to greater efficiency and consistency. Again, the clearer and more universal the law, the more organizations can focus on respecting privacy and securing data.

The U.S. needs and deserves a comprehensive federal privacy law. The stakeholders can work to find acceptable compromises to both protect personal information and ensure continued economic growth.

## Cybaris®

Cybaris®, an Intellectual Property Law Review, publishes non-student articles and student comments on all areas of intellectual property law, including patents, copyrights, trademarks, licensing, and related transactional matters.
mitchellhamline.edu/cybaris

## Intellectual Property Institute

Cybaris® is a publication of the Intellectual Property Institute at Mitchell Hamline School of Law.
mitchellhamline.edu/ip

MITCHELL | HAMLINE
School of Law


875 Summit Avenue, Saint Paul, MN 55105
mitchellhamline.edu