The Past, Present, and Future of U.S. Privacy Law

By Kirk J. Nahra[*]

[*]Kirk J. Nahra is a Partner with WilmerHale in Washington, D.C., where he co-chairs the Cybersecurity and Privacy Practice. He teaches Health Care Privacy and Security Law and Information Privacy Law at the Washington College of Law at American University. He is an adjunct professor at Case Western Reserve University Law School and the University of Maine Law School. He also serves as a fellow with the Cordell Institute for Policy in Medicine & Law at Washington University in St. Louis and as a fellow with the Institute for Critical Infrastructure Technology.

I. INTRODUCTION

Despite its antecedents in one of the most widely cited law review articles of all time from more than 130 years ago,[1] modern United States privacy law is roughly twenty years old. Even though still in its relative infancy, privacy law is now everywhere. It affects the daily lives of almost everyone, virtually everywhere in the world. It has implications for virtually every company, in virtually every industry, in virtually every country in the world. And the substantive provisions of privacy law are changing and evolving in real-time, with major developments essentially every year (with a future overall U.S. national privacy law as the ultimate privacy pot of gold at the end of this legal rainbow). There are few court decisions, and a lot of open issues, as regulated entities struggle to understand and apply these relatively new provisions.

As part of this evolution, the legal structure for protecting privacy in appropriate ways is one of the defining debates of our society today, with no signs of slowing down in the foreseeable future. At the same time, privacy law (in its own development) is barely a young adult. Based on its childhood and teenage periods, what will privacy law grow into as it matures and becomes a responsible member of society? As we look toward a potential national privacy law, what are the governing principles and key issues for this future law?

II. PRIVACY LAW IN ITS CHILDHOOD

A full history of privacy law is beyond the scope of any symposium article.[2] Modern privacy law certainly can be traced in large part to the "Fair Information Practice Principles," derived from the Advisory Committee on Automated Personal Data Systems of the Department of Health, Education and Welfare in the 1970s, the Privacy Protection Study Commission under President Carter, and the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data by the Committee of Ministers of the Organization for Economic Cooperation and Development in 1980.[3] In terms of federal statutes, the Fair Credit

---

[1] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Shapiro and Pearse have identified this article as the second most-cited law review article of all time. *See* Fred R. Shapiro & Michelle Pearse, *The Most-Cited Law Review Articles of All Time*, 110 MICH. L. REV. 1483 (2012).

[2] *See generally* DANIEL J. SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW (Rachel E. Barkow et al. eds., 7th ed. 2021); WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW (2016).

[3] *See* Fred H. Cate, *The Failure of Fair Information Practice Principles*, CONSUMER PROTECTION IN THE AGE OF THE INFO. ECON. (2006), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972; *see also* Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017).

Reporting Act, while not always considered a privacy law, implemented many of these principles (even before they were formally developed) when it was adopted in 1970.[4]

In terms of the true modern era, however, the core of modern U.S. privacy law begins in the mid-1990s, when Congress tried but failed to address privacy on the internet.[5] For the newly emerging privacy bar, privacy law became a relevant issue for big business (and big law firms) with the passage of the Gramm-Leach-Bliley Act in 1999 ("GLB").[6] This law—which was drafted primarily to modify Depression-era restrictions on the ability of financial institutions and insurers to cross industry lines—included specific privacy protections to protect the nonpublic financial information of financial institution consumers (primarily involving banks and insurance companies).[7] At roughly the same time, the U.S. Department of Health and Human Services began drafting the privacy rules for the Health Insurance Portability and Accountability Act of 1996[8] ("HIPAA"), which were issued in final form in 2001 and required compliance for a broad variety of health care entities in 2003. GLB and HIPAA created some patterns that have dominated U.S. privacy law since then. These laws apply to limited categories of entities in a particular industry (financial institutions for GLB and health care "covered entities" for HIPAA). They created a federal baseline, with "stricter" state laws generally permitted. The relevant rules protected "consumers" of these entities. Both laws required distribution of privacy notices to these protected individuals and provided certain rights to individuals under these notices (if the individuals read the notices, understood them, and chose to take action).

[4] *See* Fair Credit Reporting Act, Pub. L. No. 91-508, §§ 601–622, 84 Stat. 1114, 1127–36 (1970).

[5] It did manage to pass the Video Privacy Protection Act to ward off reporters from seeking video rental records of elected officials and others. *See The Video Privacy Protection Act as a Model Intellectual Privacy Statute*, *in* DEVELOPMENTS IN THE LAW: MORE DATA, MORE PROBLEMS, 131 HARV. L. REV. 1766, 1767 (2018).

[6] Gramm-Leach-Bliley Act, Pub. L. 106-102, §§ 501–527, 113 Stat. 1338, 1436–50 (1999) (codified at 15 U.S.C. §§ 6801–6827).

[7] Title V, Subtitle A of GLB addresses the privacy of nonpublic personal information by financial institutions.

[8] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, sec. 261–264, §§ 1171–1179, 110 Stat. 1936, 2021 (amending Title XI of the Social Security Act by adding Part C, codified at 42 U.S.C. §§ 1320d–1320d–8).

III. THE TEENAGE YEARS

Once these initial steps went into effect, privacy law began to expand in various directions. Data security—the physical protection of personal information—began to be regulated by law. Both GLB and HIPAA include specific security requirements for the entities subject to these laws.[9] Some states started to enter this debate as well.[10]

A separate body of law emerged, beginning in California, related to notification of individuals in the event of a security breach. The groundbreaking California law[11] was passed in 2002. Currently, every state and the District of Columbia has its own version of this kind of law (with meaningful differences from state to state).[12]

Privacy laws also began to emerge around the world. The European Data Privacy Directive went into effect early in this process, in 1995.[13] It was followed by the implementation of the General Data Protection Regulation ("GDPR") across the EU, with compliance beginning in 2018.[14] To the extent there is a primary international model, GDPR provides a baseline for many laws in other countries. Significant privacy laws exist in many other countries, with new laws being added (e.g., Brazil in 2020) or considered (e.g., in India and China) regularly.[15]

In addition to laws regulating particular industries or particular kinds of "problems," laws also began to regulate certain practices involving personal data. This includes the Telephone Consumer Protection Act (the primary source of the popular "Do Not Call" list) and

---

[9] *See* Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 (2002); 45 C.F.R. Part 160 (2000) and 45 C.F.R. Part 164, Subpart C (2003); William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1146–47 (2019).

[10] *See, e.g.,* Standards for the protection of personal information of residents of the Commonwealth, 201 MASS. CODE REGS. 17.01–04 (2009), https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the.

[11] CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2020).

[12] *See Security Breach Notification Chart*, PERKINS COIE (June 2020), https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

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

[14] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. Article 3 (L. 119) 1 (EU) [hereinafter GDPR].

[15] *See generally Data Protection Laws of the World*, PERKINS COIE, https://www.dlapiperdataprotection.com (last visited Mar. 6, 2021).

the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, regulating email marketing.[16] We also saw laws requiring specific kinds of website privacy notices.[17] In addition, data related to children (meaning under the age of 13) also received special protection in the Children's Online Privacy Protection Act.[18]

IV. GRADUATE SCHOOL

In the past few years, we have seen additional "second-level" privacy laws go into effect at both the state and federal levels. Illinois passed the Biometric Information Privacy Act ("BIPA"), which has become a leading source of privacy-related litigation.[19] Other states are following with their own biometric laws. Some states are passing "HIPAA-like" or "HIPAA-lite" laws (although these laws are confusing and both duplicate HIPAA provisions for some entities and impose similar obligations for other entities).[20] The California Consumer Privacy Act (CCPA)[21] has become a primary source of compliance attention and focus from other legislatures through a groundbreaking "all-purpose" privacy law. This law has spawned a series of amendments, several versions of regulations, and a follow-on referendum that passed in California in November 2020, all for a law that went into effect on January 1, 2020.[22] It also has led to a debate in

---

[16] Telephone Consumer Protection Act of 1991, Pub. L. No. 102-243, § 3(a), 105 Stat. 2394 (codified at 47 U.S.C. § 227); Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 15 U.S.C. §§ 7701-13).

[17] California Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE §§ 22575-79 (West 2014) (even though website privacy notices have become a general best practice). California has long been a pioneer in privacy law, although many of its laws have not been implemented in other states. *See* Kirk J. Nahra, *What's Up With California?,* 3 BNA PRIVACY & SEC. L. 72, 72–74 (Jan. 19, 2004), http://www.ehcca.com/presentations/HIPAA9/nahra_h2.pdf.

[18] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105–277, §§ 1301–1306, 112 Stat. 2681–728, 728–35 (codified at 15 U.S.C. §§ 6501–6505).

[19] *See, e.g.*, Rosenbach v. Six Flags Entm't Corp., 129 N.E.3d 1197 (Ill. 2019); Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

[20] Confidentiality of Medical Information Act, CAL. CIV. CODE §§ 56–56.37 (West 2021); Texas Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE ANN. §§ 181.001–207 (West 2019).

[21] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–199, https://theccpa.org (containing original text plus legislative amendments to date).

[22] See CALIFORNIA CONSUMER PRIVACY ACT, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (WEST) (version of the CCPA that passed the California legislature in 2018); Cal. Civ. Code §§ 1798.00-1798.199 (version of the CCPA currently enacted into law); 11 CCR §§ 999.300-999.337 (implemented CCPA regulations by the California Attorney General's office); Proposition 24 (California Privacy Rights Act) (Nov. 3, 2020), available at https://www.oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28

states across the country about their own state laws, although (as of the drafting of this article) no other states have passed a comprehensive privacy law since then.[23] One result of these laws is increased complexity of the regulatory structure, with potentially negative implications for businesses attempting to comply and for consumers trying to understand their rights.

Then COVID-19 hit. Attention to broader privacy laws at the state and federal levels ceased. And COVID-19 raised a variety of new issues for debate in the overall privacy context, making the overall discussion even more complicated.[24]

V. EVOLVING INTO AN ADULT PROFESSIONAL

Despite the volume of privacy laws in the United States, there is widespread criticism of the current privacy structure. The EU has not found the U.S. Privacy system to be "adequate," meaning that there are real challenges to the transfer of data from the EU to the U.S. The notice and choice approach has failed.[25] The fair information practices themselves have failed.[26] There are growing gaps in the regulation of personal data by sector, as the industries defined (for example) by HIPAA and GLB have expanded beyond the lines drawn by the legislature.[27] There are increasing regulatory challenges for businesses and growing confusion for consumers.

Consumer%20Privacy%20-%20Version%203%29_1.pdf (ballot initiative that further amended the CCPA).

[23] Some examples of state proposals include: Press Release, Shelley Kloba, Wash. State Rep., People's Privacy Act Introduced in Washington State House of Representatives (Feb. 1, 2021) (on file with author); Press Release, Okla. House of Reps., Bipartisan Data Privacy Legislation Filed (Jan. 20, 2021) (on file with the Okla. State Leg.); H.B. 2307, 2021 Sess. (Va. 2021) (Virginia Consumer Data Protection Act).

[24] Kirk Nahra, *The Pandemic and the Evolution of Health Care Privacy*, INT'L ASS'N OF PRIVACY PROF'LS (May 6, 2020), https://iapp.org/news/a/the-pandemic-and-the-evolution-of-health-care-privacy.

[25] Professor Woodrow Hartzog, for example, has called the notice and choice model "irreparably broken," because the control it promises users is "an illusion" and the "dizzying array of switches, delete buttons, and privacy settings" is "overwhelming." *Policy Principles for a Federal Data Privacy Framework in the United States: Hearing Before the S. Comm. on Commerce, Sci., & Transp.*, 116th Cong. 3–4 (2019) (statement of Woodrow Hartzog, Professor of Law & Computer Science, Northeastern University).

[26] *See generally* Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343 (Jane K. Winn ed., 2006); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952 (2017).

[27] *See, e.g.*, Kirk Nahra, *Moving Toward a New Health Care Privacy Paradigm*, (November 2014), https://www.healthit.gov/sites/default/files/facas/PSWG_Background_Kirk_Nahra_Health_Care_Privacy_Paradigm_2014-12-08.pdf; *The Data Will See You Now*, ADA LOVELACE INST. (2020).; U.S. DEP'T OF HEALTH AND HUMAN SERVICES,

So where do we go from here?

The CCPA has kicked off a meaningful debate about state privacy law—but there is little to show for this debate (yet). While we can expect other states to follow California's lead (even if not the overall approach of the CCPA and its younger sibling, the California Privacy Rights Act),[28] this debate and meaningful progress have been slow.

The federal debate also is moving along, slowly but steadily. We have seen a variety of proposed bills, Congressional hearings, industry and advocacy group white papers, and position statements, all of which are intended to influence an eventual national privacy law. When thinking about this law, what are the key issues to be discussed and included in this law?

A. *Preemption*

Preemption of state law has become topic one in the current debate about a national law. The question is whether the federal law will create only a baseline minimum standard, while allowing state law to provide greater protection for individual privacy, or whether the federal law will take the place of all state laws.[29] For corporate America, this is an enormously important issue. At this point, there are meaningful partisan differences on this issue, with Democrats generally allowing state law to provide greater rights and Republicans favoring a single federal standard.[30]

B. *Private Right of Action*

The second critical issue that has been occupying a meaningful portion of the national debate involves whether there will be a private cause of action for violations of the federal law. Democrats lean toward permitting a private cause of action, and Republicans do not generally support one. There are a variety of "intermediate" possibilities here, including providing a private right of action only in specific, defined situations, allowing state Attorneys General to enforce the privacy law

Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA (June 2016).

[28] The California Privacy Rights Act of 2020 (amending Cal. Civ. Code §§ 1798.100–199.100 (2018)).

[29] *See* Cameron F. Kerry & John B. Morris Jr., *Preemption: A Balanced National Approach to Protecting All Americans' Privacy*, THE BROOKINGS INST. (June 29, 2020), https://www.brookings.edu/blog/techtank/2020/06/29/preemption-a-balanced-national-approach-to-protecting-all-americans-privacy.

[30] Peter Swire & Pollyanna Sanderson, *A Proposal to Help Resolve Federal Privacy Preemption*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 13, 2020), https://iapp.org/news/a/a-proposal-to-help-resolve-federal-privacy-preemption.

as well (which may help navigate both this issue and the preemption issue), only permitting claims for damages in specific situations, or not permitting class action claims.[31]

C. *Existing Federal Laws (and Whether and How They Will Still Apply)*

Preemption and a private cause of action have taken up most of the oxygen in the national debate to date. This means that most of the substance of a national law remains up for debate. In this regard, one critical question involves how a new federal privacy law will treat the existing federal privacy laws, both those involving specific sectors and those involving particular practices.

The health care example is illustrative. The HIPAA privacy and security rules address privacy and security protections for certain defined elements of the health care system (mainly the activities of health care providers and health insurers). There has been tremendous growth in recent years in the creation and collection of "non-HIPAA" health data, gathered by entities outside the reach of the HIPAA statute. At the same time, there has been an enormous expansion in the use by the health care industry of "non-health" data—elements such as income, marital status, voting patterns, shopping habits, and television habits—for a variety of health care purposes. This has created meaningful gaps in the protection of true health information, and blurred lines between health and non-health data.

The effort at the state level to address these issues has been problematic. Some state laws[32] create state versions of the HIPAA rules—with overlaps in coverage and expanded coverage in vague settings where the expansion may make little sense.

---

[31] *See generally* Cameron F. Kerry & John B. Morris Jr., *In Privacy Legislation, a Private Right of Action is Not an All-or-Nothing Proposition*, THE BROOKINGS INST. (July 7, 2020), https://www.brookings.edu/blog/techtank/2020/07/07/in-privacy-legislation-a-private-right-of-action-is-not-an-all-or-nothing-proposition; Joseph Jerome, *Private Right of Action Shouldn't be a Yes-No Proposition in Federal US Privacy Legislation*, INT'L ASS'N OF PRIVACY PROF'LS (Oct. 3, 2019), https://iapp.org/news/a/private-right-of-action-shouldnt-be-a-yes-no-proposition-in-federal-privacy-legislation.

[32] *See supra* note 20.

The CCPA took a different approach. Despite being viewed as an "all-purpose" privacy law, the health care information of California residents is covered by at least six different regulatory structures:

1. HIPAA protected information (generally exempted from CCPA);
2. CMIA covered companies/information (generally exempted from CCPA);
3. Common Rule/Clinical research data (generally exempted from CCPA);
4. CCPA—covers health information if it is not otherwise exempted;
5. but CCPA does not cover health data held by non-profits;
6. and CCPA does not generally cover health data held by employers about their employees.

The resulting structure in California appears to be a "lose-lose"—companies must navigate regulatory lines that have little to do with actual behavior, and consumers have no realistic way to understand these very different structures.

The approach taken in Europe under the GDPR provides an alternative model. All data is protected in virtually all settings—including health information—regardless of who holds it. True health data is treated as "sensitive" data—along with other sensitive data categories, including data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, or data concerning a natural person's sex life or sexual orientation—and receives additional protections with this status. But the nuance present in the HIPAA rules—which is designed to balance a variety of goals and interests, and to generally protect privacy while at the same time permitting the health care system to work effectively—is entirely absent in GDPR. That makes GDPR an alternative, but it is not really a better model if the goal is better privacy and a working health care system.

Accordingly, this question of how to address these existing laws is tremendously important. They could be supplemented or replaced, or the currently covered entities could simply be left alone.[33]

[33] *See* Kirk J. Nahra, *Healthcare in the National Privacy Law Debate*, AMERICAN BAR ASS'N (Dec. 5, 2019); Kirk J. Nahra, *The New HIPAA NPRM—The Latest and Greatest in the Evolution of the HIPAA Privacy Rule*, AMERICAN HEALTH L. ASS'N HEALTH L. WKLY (December 18, 2020) (discussing how the HIPAA rules may need modification to address health care system evolution).

D. *Enforcement*

Enforcement of U.S. privacy law currently is dispersed across a wide number of government agencies. Many of the laws designate a specific enforcement agency. For example, the U.S. Department of Health and Human Services' Office for Civil Rights is the primary enforcement agency for HIPAA. Various federal agencies with defined regulatory authority enforce the Gramm-Leach-Bliley Act (along with state insurance departments for insurers not subject to federal law). State attorney generals have broad enforcement authority over privacy and security in general, both through specific laws, like data breach notification laws, and through their general authority over consumer protection. The U.S. Department of Justice often has criminal authority in particularly egregious situations.

In addition to specific agencies, the Federal Trade Commission (FTC) has a "catch-all" authority on privacy and security practices. The basic consumer-protection statute enforced by the FTC is Section 5(a) of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce. Generally, misrepresentations or deceptive omissions of material fact constitute deceptive acts or practices and are thus prohibited by Section 5(a) of the FTC Act. Also, acts or practices are deemed unfair under Section 5 of the FTC Act if they cause, or are likely to cause, substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or the competition. The FTC has acted in multiple cases involving data security and conducts a wide range of investigations into privacy practices across industries.[34]

Despite its range of activities, the FTC has various meaningful limitations on its actions. The statute—enacted in 1914—obviously was not directed to privacy and security concerns. In addition, as a broad generalization, the FTC typically does not have authority to issue fines in the first instance under Section 5; rather, the "typical" FTC settlement involves an agreement to engage in the behavior that the FTC believes should be in place in any event, such as an agreement to implement a reasonable and appropriate security program.[35] Some FTC

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

[35] *See, e.g.*, *In re* Uber Technologies Inc., FTC Decision and Order (Docket No. C-4662), Oct. 25, 2018 (requiring the company to "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of [personal information]"); In the Matter of Lightyear Dealer Technologies, FTC Decision and Order (Docket No. C-4687), Sep. 6, 2019 (preventing the

Commissioners—particularly (now former) Commissioner Chopra and Commissioner Slaughter—have been advocating for more aggressive action by the FTC.[36] Others believe that the FTC can only engage in "appropriate" enforcement activities—consistent with a broader view of privacy enforcement—with legislative changes from Congress.[37] Some—in Congress and elsewhere—believe that the FTC should be replaced as the primary privacy and security regulator with a specific agency for that purpose, modeled on the data protection agencies in Europe.[38]

E. *Scope of Individual Rights*

Both GDPR and the CCPA have introduced a wider vision of individual rights that should apply to personal data, including the right to access, the right to correct, the right to amend, even the right to delete. GDPR incorporates individual rights as a supplement to the core controls on how an entity can use and disclose (or "process" personal data to use GDPR language), while CCPA's focus is almost entirely on these individual rights. Individual rights are also important under the HIPAA rules—although not frequently exercised by individuals. Particular attention has been paid to the HIPAA access right in recent years, both in policy debates and in enforcement.[39] CCPA adds a new

company from selling, sharing, collecting or maintaining personal information unless it "establishes and implements, and thereafter maintains, a comprehensive information security program . . . that protects the security, confidentiality, and integrity of such [information]").

[36] *See, e.g.*, Fed. Trade Comm'n, Dissenting Statement of Comm'r Rohit Chopra Regarding Zoom Video Communications, Inc., Commission File No. 1923167 (Nov. 6, 2020); Fed. Trade Comm'n, Joint Statement of Comm'r Rohit Chopra and Comm'r Rebecca Kelly Slaughter Concurring in Part, Dissenting in Part *Regarding In the Matter of Flo Health, Inc*., Commission File No. 1923133 (Jan. 13, 2021); Feb. Trade Comm'n, Statement of Comm'r Rohit Chopra regarding *In re Everalbum and Paravision*, Commission File No. 1923172 (Jan.8, 2021); and Fed. Trade Comm'n, Statement of Comm'r Rohit Chopra Joined by Comm'r Rebecca Kelly Slaughter Regarding *In the Matter of Tapjoy, Inc*., Commission File No. 1723092 (Jan. 7, 2021).

[37] Chris J. Hoofnagle, Woodrow Hartzog & Chris J. Solove, *The FTC Can Rise to the Privacy Challenge, But Not Without Help from Congress*, THE BROOKINGS INST. (AUG. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

[38] *See, e.g.*, Press Release, Sen. Kirsten Gillibrand, Confronting a Data Privacy Crisis, Gillibrand Announces Landmark Legislation to Create a Data Protection Agency (Feb. 13, 2020) (on file with author).

[39] The "interoperability" rules of the 21st Century Cures Act are designed to facilitate an individual's right to access their health information. Press Release, HHS Press Office, HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data (March 9, 2020) (on file with author). The recent NRPM under the HIPAA rules also focused on expanding and clarifying this access right. *See* Kirk J. Nahra, *The New HIPAA NPRM—The Latest and Greatest in the Evolution of the HIPAA Privacy Rule*,

right—the right to opt-out of the sale of personal data—which has created meaningful compliance complications along with the benefits to individuals. At the same time, this may have inadvertently threatened certain programs, such as loyalty programs that often provide certain direct benefits to consumers.

F. *Permitted Disclosures vs. Areas Where Permission from Consumers is Needed*

Another key issue involves the underlying rules for how a covered company can use and disclose the personal data that will be subject to a law. Today, in most settings in the U.S., the core approach is that where a privacy notice discloses a particular kind of use or disclosure, that use or disclosure is permitted consistent with the "notice and choice" framework. There are some exceptions, but this rule governs most personal data today in most settings, particularly in sectors unregulated by existing sector laws. By comparison, GDPR imposes specific obligations on companies before personal data can be processed. The HIPAA rules do the same, creating areas where data can be disclosed with relative ease (related to "treatment," "payment," and "health care operations" as defined by the HIPAA Privacy Rule), where use and disclosure are permitted for public policy reasons. For all other purposes, HIPAA requires individual authorization.[40]

The HIPAA approach—which focuses on the "context" of how data is collected, used, and disclosed—represents a useful approach.[41] It is particularly effective for the health care industry, where appropriate balances are needed to accomplish a broad variety of goals in addition to protecting privacy rights. The challenge going forward—if Congress chooses to define these appropriate uses and disclosures rather than rely primarily on notice and choice—is how to define the appropriate context for all industries and all purposes. Describing what is "typical" or "normal" or "expected" for health care financial services may be much easier than crafting what addresses retail, social media, education, employment, and the broad, and perhaps unlimited, range of other categories of users of personal data.

AM. HEALTH L. ASS'N HEALTH L. WEEKLY (December 18, 2020). In recent years, the HHS Office for Civil Rights has engaged in a significant series of enforcement matters related to the right to access. *See* Press Release, HHS Press Office, OCR Settles Fourteenth Investigation in HIPAA Right of Access Initiative (Jan. 12, 2021) (on file with author).

40 45 C.F.R. § 164.506 (2013).

41 Kirk J. Nahra & Lydia Lichlyter, *Federal Privacy Legislation Should Be Context-Sensitive*, LAW360 (February 27, 2020).

G. *Scope of Personal Data*

The concept of "personal data" has evolved significantly during the modern era of privacy. Moving beyond concerns primarily for addresses and contact information, internet profile data became critical for the blossoming online advertising industry. Personal devices moved these identifiers from a desktop environment to a variety of additional situations. The Internet of Things developed all kinds of new information that might be associated with an individual or connected to a specific person's activity, even if the identity of that person was not known to the advertiser.

Today, laws such as CCPA and GDPR define personal information in very broad ways, intending to "future proof" these definitions as technology evolves (for example, the CCPA includes as personal information "olfactory" information, which in my experience is not yet used as a personal identifier, but certainly could be in the future). Separate from this identification aspect, there also are key questions on the scope of categories of individuals who would be protected by such a law. GDPR applies to all individuals. CCPA excludes (for the most part) data about employees and personal data about individuals that are obtained in a business-to-business setting (e.g., company A has the email and phone number of an employee of company B because of business dealings between company A and company B). Will a federal privacy law include these categories of individuals?

H. *Special Protection for "Sensitive" Data (and How is That Defined)*

Some privacy laws provide special protection for particular categories of data, usually identified as "sensitive" data categories. Will the U.S. privacy law identify particular categories of data that are worthy of special protection? The EU identifies certain data categories as "sensitive," including certain data elements not necessarily given any special consideration in the U.S. (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or data concerning a natural person's sex life or sexual orientation). State data breach notification laws identify particular categories of data that justify data breach notification (such as a Social Security Number). The HIPAA rules generally treat all health information at the same level of sensitivity—meaning that not only is your address protected in the same way as your medical information, but information about foot surgery receives the same level of protection as information about your mental health or HIV status. It is clear that what is sensitive in some contexts, or to some people or in some countries, is not always sensitive.

Information that a patient went to a general practice physician may not be sensitive, but any indication of a visit to a psychiatrist might be. Accordingly, identifying these categories of data, defining them in useful and practical ways, and then identifying what additional protections will be given to this data is a significant challenge.

I. *Intention Toward International Principles*

Conceptually, one of the driving forces behind a U.S. national law involves international comity issues. Many privacy laws in other countries outside the U.S. impose obligations and restrictions on the transfer of personal data out of those countries. Some countries impose "data localization" requirements that prohibit this data from leaving the country. Other international frameworks (e.g., the European Union) permit transfers, but only to countries with "adequate safeguards"—of which the U.S. currently is not one.[42] So, will a U.S. law reach a sufficiently high level of personal data protection that it will meet these international standards?

J. *Discrimination/Artificial Intelligence/Algorithms/Big Data*

There has been enormous attention paid in recent years to the potentially discriminatory impact of big data analytics and the use of artificial intelligence. Many of these concerns involve potential or perceived adverse impacts based on "neutral" algorithms, and the increasing recognition of risks in the development of these algorithms.[43] A key question in the U.S. national debate is whether these discrimination principles will be addressed in a national privacy law. Personal data—although not always identifiable to an individual—is essential to the development of these algorithms. At the same time, at least in the U.S., these risks typically have been addressed in the context of "civil rights" laws or other substantive provisions (regulating insurance, financial services, housing, and the like) rather than through privacy laws. Will the drafters of a national privacy law try to tackle this

[42] This data transfer element is creating enormous contemporary concerns today, with mechanisms for appropriate data transfer from Europe to the U.S. dwindling rapidly in the wake of the Schrems II decision in the summer of 2020. *See, e.g.*, Joshua P. Meltzer, *The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security*, THE BROOKINGS INST. (August 5, 2020), https://www.brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security; Kenneth Propp & Peter Swire, *Geopolitical Implications of the European Court's Schrems II Decision*, LAWFARE (July 17, 2020), https://www.lawfareblog.com/geopolitical-implications-european-courts-schrems-ii-decision.

[43] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (2015).

issue in the privacy law? Addressing issues raised by these questions are critical to the future of U.S. law—but including them in a privacy law may be both unnecessary and create enormous new complications for an already complicated set of core privacy issues.

K. *Data Security Issues*

There have been separate efforts for several years to pass a national law addressing data security requirements. Some of these efforts preceded the current privacy debate (and moved further in the legislative process than privacy has done to date), but these efforts at a national standard for data security did not pass. Will they resurface in a national privacy law?

L. *Data Breach Notification*

Similarly, there were efforts to pass a national law related to data breach notification. In part, this effort was driven by a number of states that—at the time—did not have state versions. Now every state has a data breach notification law. A national law would only be useful at this point if it were to standardize the approach for data breach notification by creating a national standard and preempting the fifty different state laws.

VI. CONCLUSION

Privacy law is now a primary area of activity across the legal structure. It is an essential skill for law students.[44] It is creating tremendous professional opportunities for law students and lawyers across the country and around the world. Privacy law also is at the forefront of a broad variety of public policy debates, ranging from the development of artificial intelligence and algorithms to facial recognition and the role of social media in our political process. Data is the engine that is driving commerce around the world—so much so that data practices of large tech companies are now leading Congress and others to investigate technology companies for antitrust violations based on their data activities. The Internet of Things is leading a wide range of industries to now view data gathering and analytics as a primary mode of behavior, from car companies to refrigerators to smart speakers and even sex toys. We are engaged in a broad national debate over these privacy issues, and privacy lawyers will be following this debate carefully as it inches forward toward a U.S. national privacy law.

[44] Kirk J. Nahra, *Privacy Law and the First-Year Law School Curriculum*, 23 GREEN BAG 2D 21, 22 (Autumn 2019).

There is an opportunity to create a comprehensive U.S. national privacy law. That law would serve—at a minimum—to create enforceable standards that fill in the gaps of the existing sectoral and practice-specific structure. Today's environment both creates substantial compliance challenges—by permitting overlapping and often inconsistent requirements, and driving behavior based on the happenstance of the application of specific laws—while also leaving much personal data essentially unregulated.

Yet this idea of "filling in the gaps" is too simplistic to be useful. The issues I have identified above are each quite complicated. Evaluating them thoroughly and appropriately may be beyond the capability of Congress. Some of the judgments are both critical and largely unexamined at this point—particularly the idea of how a new privacy law should interplay with both state law (the preemption issue) and, perhaps equally as important, all the other federal laws on point. There clearly are values to simplicity in this area—both for consumers and regulated entities. Today's structure may primarily benefit privacy lawyers (I am not complaining about this). But we should be pursuing a comprehensive law that provides meaningful consumer protections that are understandable, but at the same time, imposes obligations on corporate entities that provide realistic and appropriate restrictions while still permitting efficient cooperation of those permitted activities. The focus should be on defining certain key concepts, and then creating straightforward rules to guide behavior, inform consumers, and provide useful measuring sticks for reasonable enforcement.