PROGRAMMING DIGITAL PRIVACY INTO PUBLIC POLICY:

A New Rule of Law Through Legislative Action

By Jeff D. McAlpin

Legal stability is cited as a fundamental characteristic of the rule of law.[1] At the same time, a body of law, to maintain long-term viability, must be able to cope with novel situations, including new legal relationships and technologies. These two characteristics emblematic of the rule of law, predictability and adaptability, coexist under tension with each other. In common-law jurisdictions, the tension is resolved by relegating to the domain of private law "everyday tort, contract and property cases" and deciding them based on precedent, which is "open to modification."[2] On the other hand, irrespective of whether a governmental entity is a common-law or civilian jurisdiction, changes to its public law are most often accomplished through legislation, with the political process balancing the impetus for change against the value of stability.

To Louisiana civilians, this is a familiar process, as in Louisiana the Legislature is the source of law both public and private. For digital-privacy regulation, now a public policy question, the tension between consumer advocates seeking new protections and business interests requiring the predictability of clear regulatory guidance is being mediated through the legislative process at the state, federal and international level.

As of November 2022, no singular federal law regulates digital privacy. This article summarizes the history of the right to privacy and then provides a snapshot of the rapidly evolving landscape of state data-privacy regulation. It also discusses pending federal privacy legislation, noting objections to its passage and contrasting it with legislation in the European Union. Lastly, this article highlights the regulatory burdens of digital-privacy legislation from a business perspective, including actionable steps companies with access to consumer digital information can take in preparing compliance plans amidst the kaleidoscope of state legislation.

A Brief History of Privacy

In 1890, Samuel D. Warren and Louis D. Brandeis (ranked second and first in their graduating classes at Harvard Law School in 1877, respectively) published "The Right to Privacy" in the *Harvard Law Review*.[3] The Harvard article traced, through the centuries, the development in the common law of new rights based on old rights. The development of new technologies, such as photography and audio recording, led to new media with mass dissemination of image and sound. Through these new media (tabloid newspapers, for example), the private, domestic affairs of non-public figures were brought with new immediacy into the public eye.[4]

In 1965, the Supreme Court in *Griswold v. Connecticut* first recognized privacy as a right, albeit a right not specifically guaranteed in the Constitution. Justice Douglas' majority opinion characterized the right to privacy as "penumbras," gray shadows formed by emanations from "specific guarantees in the Bill of Rights."[5] *Roe v. Wade* in 1973 cited *Griswold* when finding a liberty interest as the foundation for a right to privacy in reproductive decisions but ultimately relied on incorporation through the Due Process Clause of the Fourteenth Amendment.[6] Cases after *Roe*, but before the *Dobbs* decision, also typically grounded the right to privacy not in a penumbral theory but under the substantive Due Process Clause of the Fourteenth Amendment.[7]

The Supreme Court overruled *Roe* and later cases on abortion in June 2022 with *Dobbs v. Jackson Women's Health Organization*, observing that the right to abortion was unknown at the time of the adoption of the Fourteenth Amendment. Justice Alito's majority opinion in *Dobbs*, centering its analysis on what rights were recognized at the time of the Fourteenth Amendment's adoption in 1868, calls into question whether other previously recognized privacy rights will continue to enjoy constitutional protection.[8]

In contrast to the Constitution of the United States, many state constitutions explicitly state a right to privacy among the individual rights recognized by the state.[9] Many amendments adding a right to privacy to state constitutions were passed in 1970s, a time of public concern about how the creation and use of computerized databases might impact individuals' privacy rights.[10] Coupled with this constitutional recognition, state legislative implementation of enforcement mechanisms afforded protection under law of the privacy rights of citizens. Public concern also led to federal legislation. The Privacy Act of 1974 established a code of fair information practices governing the collection, maintenance, use and dissemination of information about individuals by federal agencies.[11] Exceptions to the statute include information compiled (1) in anticipation of civil litigation, (2) by the CIA and (3) for agency use pertaining to criminal law enforcement.[12]

Current State of Digital Privacy Regulation: State, Federal and International

Indeed, the current landscape of federal data-privacy regulation is not so much a vacuum as a miscellany, complete with acronyms: the Health Insurance Portability and Accountability Act (HIPAA); the Fair Credit Reporting Act (FCRA); the Family Educational Rights and Privacy Act (FERPA); the Gramm-Leach-Bliley Act (GLBA); the Electronic Communications Privacy Act (ECPA) (from 1986 and ill-suited to the modern Internet, redefined to large extent by the USA Patriot Act); the Children's Online Privacy Protection Rule (COPPA) (imposing data-collection limits for children under 13 years of age); the Video Privacy Protection Act (VPPA) (a reaction after the video-rental history of Supreme Court nominee Robert Bork was obtained by a journalist, but held not to apply against streaming companies); and the Federal Trade Commission Act (FTC Act) (allowing the FTC to go after apps or websites that violate their own policies or terms of their marketing language).[13]

Amidst this alphabet soup is a state law landscape that is constantly evolving. Five states (California, Colorado, Connecticut, Virginia and Utah) have signed digital-privacy legislation.[14] California's law first became effective in 2020, while the other four states with

signed legislation became or will become effective on various dates in 2023. Four other states (Michigan, New Jersey, Ohio and Pennsylvania) have active bills as of November 2022. The status of those bills is uncertain and underscores a larger uncertainty as to the future of data-privacy legislation on a state-by-state basis, especially with respect to national companies that must comply with those laws.

A brief overview of the consumer protections provided by data-privacy regulations in California and the European Union is useful before exploring the pending federal data-privacy regulation and obstacles to its passage.

Consumer-advocacy groups consider California's state law, the California Consumer Privacy Act (CCPA), as enhanced by amendments effective Jan. 1, 2023, to afford the most protection of any current state law.[15] Among its basic privacy rights, the CCPA gives consumers (1) the right to know about the personal information a business collects about them and how it is used and shared; (2) the right to delete personal information collected from them (with some exceptions); (3) the right to opt-out of the sale of their personal information; and (4) the right to non-discrimination for exercising their CCPA rights.[16] Under the act, businesses must give consumers notice explaining their privacy practices. The notice requirement applies to data brokers and many other businesses, not just businesses that collect digital information directly from consumers.

The European Union Parliament passed data-privacy regulation, termed the General Data Privacy Regulation (GDPR), in April 2016, effective on May 5, 2016, and transposed into the national law of EU countries by a May 6, 2018, deadline.[17] The GDPR has five major aspects: (1) The law requires data inventory, or mapping, which means companies must document how all personal data is used, managed, processed and shared. (2) Individuals have the right to learn more about what data a company possesses. This right includes a "writ of habeas data," where companies are required to provide all information they possess related to an individual. The individual also has the right to amend that data or demand the company delete it if the individual does not want the company to have it. (3) Third-parties or vendors must be managed by companies subject to jurisdiction under the act for security and to mitigate against the risk of data breaches. (4) A requirement of privacy by design, where new technologies, new business processes or new uses of personal data must also provide privacy protections. (5) Companies must identify specific individuals to be responsible for privacy at that company.[18]

Further, there are conflicts-of-law issues where the GDPR may grant fewer or more protections than the constitutions or laws of member states of the EU. The risks to U.S. companies associated with non-compliance of the GDPR are substantial: in 2021, Amazon, Meta and Google were levied penalties of over $100 million in the aggregate, and the data indicates both the individual number and aggregate amount of fines increased in 2022.[19]

Obstacles to Uniformity Through Federal Regulation: Conflict Between Consumer and Business Interests

Policy questions around the proposed federal legislation, the American Data Privacy and Protection Act (ADDPA), implicate both California and EU law.[20] Although a detailed analysis of ADPPA's specific provisions are beyond the scope of this article, considering they may be amended during 2023 as part of legislative compromise, the Congressional Research Service has provided an overview of the act, including a summary of the bill and a comparison to existing federal privacy legislation.[21] The federal bill would grant similar (but not identical) protections to the California law while its enforcement mechanisms would be markedly different. Congressional representatives, including former Speaker of the House Nancy Pelosi, have opposed passage of the bill in its current form, citing concerns that it will preempt existing California law and offer less protection and enforcement to consumers.[22] The preemption provisions of the ADDPA would prevent states from enacting new data-privacy laws in reaction to changes in the use of data by companies brought about by technological advances.[23]

One solution to this legislative stalemate is similar to the waiver granted by the Clean Air Act of 1967, in which California was authorized to set its own vehicle-emissions standards; under such a waiver, the ADDPA could include provisions that California digital-privacy regulation was not preempted by the federal law.[24] Arguments for affording California special treatment cite that the state is the epicenter of technological innovation (*i.e.*, Silicon Valley) and the situs of the headquarters of many of the largest technology companies. This solution is speculative, as of late 2022, and the future of the federal legislation and whether California will be granted a preemption waiver to facilitate passage of the bill remain uncertain.

The need for federal regulation in this area is arguably less uncertain. Over the last two years, state regulation has been an evolving patchwork, exacerbated not only by the existence of multiple jurisdictions but also by the rapid pace of change inherent in digital technologies. Navigation of state regulations is daunting, especially from the perspective of businesses. For these businesses subject to regulation by digital-privacy acts, the costs of compliance are non-negligible, even under one regulatory regime.[25] Regulatory burdens from multiple states, with each state having different requirements, would cost, in their aggregate, a greater amount than the single cost of compliance with one, nationwide regulatory system.

Preparation Is Still Possible in the Shadow of Regulatory Uncertainty

In the meantime, companies should develop compliance plans with one eye to the applicable state and international regulatory landscapes and another eye to the proposed federal rules. Industry associations for specific areas of the law can be a source of guidance.[26] Those companies not subject to the jurisdiction of the CCPA or the GDPR may still be in the favorable position to prevent rather than cure non-compliance.

Under the assumption that new data-privacy legislation will apply to any company that does business in those states, compliance plans should address several key areas. As an initial step, legal departments should have letters ready with a legal reason not to comply with the request. Second, a business should develop a process for opt-out requests. A process-focused approach would include clearly defining the standard channel to complete a task and the creation of forms to use in the process.

To ensure compliance with the law, a company will need to follow a multi-step process. First, a company should internally map its data, making special notes of where it stores personal consumer information (including any inferences drawn from consumer information to create a consumer profile). A complete map will include how the company collects data; why, when and where it is stored; how long the data is retained; whether it is "writeable" (*i.e.*, capable of modification or deletion); and whether it is shared with any third parties. Then, contracts with third parties, including employees and service providers, should be drafted to include language on data-privacy rights (including such rights as the right of consumers to request their data, amend it and order it deleted). Finally, the company should check regulatory requirements against both the map of the company's data and the language of its contracts. Only by performing a cross-check among all three areas can the company ensure it complies with the law.[27]

Irrespective of the ultimate shape of digital-privacy legislation, it is safe to assume that it bears the continued close attention of stakeholders in business as well as consumers and their advocates. The advantage to be gained through preventative measures, seeking to anticipate a regulatory environment that is not yet present, must be weighed against the substantial compliance costs to companies. As these consumer protections move into a previously unregulated sphere of human endeavor, the rule of law will, as it always has, replace a chaotic environment, full of opportunity and hazards, with a measure of certainty. The unique certainty and protection of rule of law is the hallmark of the world's strongest free and thriving economies. In the digital economy, as it was in earlier emergent economies, the benefits of the law's prescribed rights will come at the cost of its prescribed responsibilities.

FOOTNOTES

1. Stefanie A. Lindquist & Frank C. Cross, *Stability, Predictability, and the Rule of Law:* Stare Decisis *as Reciprocity Norm*, Conference Paper, Univ. of Tex. Sch. of L., Conference on Measuring the Rule of Law (2010), *https://law.utexas.edu/conferences/measuring/The%20Papers/Rule%20of%20Law%20Conference.crosslindquist.pdf.*

2. Maimon Schwarzschild, "Keeping it Private," 44 San Diego L. Rev. 677, 677-78 (2007).

3. Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 Harv. L. Rev. 193 (1890).

4. *See,* Matthew L. Bycer, *Understanding the 1890 Warren and Brandeis "*The Right to Privacy*" Article*, Nat'l Juris Univ., *https://nationalparalegal.edu/UnderstandingWarrenBrandeis.aspx* (last visited Dec. 24, 2022).

5. Griswold v. Connecticut, 381 U.S. 479, 483-84 (1965). Among the specific provisions relied upon by Griswold are the freedom of association in the First Amendment, the Third Amendment (prohibiting quartering of soldiers), the Fourth Amendment, the Self-Incrimination Clause of the Fifth Amendment and the Ninth Amendment (reserving rights unenumerated in the Bill of Rights to the people).

6. Roe v. Wade, 410 U.S. 113, 153 (1973).

7. Lawrence v. Texas, 539 U.S. 558 (2003) (holding that Texas statutes criminalizing homosexual conduct as unconstitutional based on a liberty interest under the Due Process Clause); Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833, 846 (1992).

8. Dobbs v. Jackson Women's Health Org., 142 S.Ct. 2228, 2246-48 (2022).

9. *See, e.g.*, La. Const. of 1974, art. I, § 5 (1974) ("Every person shall be secure . . . against . . . invasions of privacy."); Cal. Const., art. I, § 1 (am. 1974) ("All people are by nature free and independent and have inalienable rights. Among these are . . . privacy."); Alaska Const. (amended 1972) ("The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section.").

10. Electronic Privacy Information Center, *https://epic.org/the-privacy-act-of-1974/* (last visited Dec. 24, 2022).

11. 5 U.S.C. § 552a (2022).

12. Office of Privacy & Civil Liberties, *Ten Exemptions*, Overview of the Privacy Act of 1974 (2020 ed.), available at *https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/exemptions* (last visited Dec. 24, 2022); *see also,* U.S. Dep't of Just., *Overview of the Privacy Act of 1974* (2020 ed.) (comprehensive treatise of existing Privacy Act case law).

13. Thorin Soskowski, "The State of Consumer Data Privacy Laws in the US (and Why It Matters)," Wirecutter (Sept. 6, 2021), *https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.*

14. Anhoky Desai, *US State Privacy Legislation Tracker*, Int'l Ass'n of Privacy Prof'ls (Oct. 7, 2022), *https://iapp.org/resources/article/us-state-privacy-legislation-tracker/*. Click "View Chart."

15. Cal. Civ. Code §§ 1798.100-199 (West 2022).

16. Rob Bonta, Cal. Dep't of Just., Office of the Atty. Gen., *California Consumer Privacy Act* (CCPA), *https://oag.ca.gov/privacy/ccpa* (last visited Dec. 24, 2022).

17. Full text pdf: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679*; *see also*, *https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en* (last visited Nov. 1, 2022).

18. Wendell J. Bartnick et al., "Present and Future Data Privacy Outlook." 24 Currents: J. Int'l Econ. L. 70, 71 (2020).

19. *https://www.enforcementtracker.com/* (last visited Nov. 1, 2022).

20. H.R. 8152, 117th Cong. (2d Sess. 2022), available at *https://www.congress.gov/117/bills/hr8152/BILLS-117hr8152ih.pdf.*

21. Congressional Research Service, *Overview of the American Data Privacy and Protection Act, H.R.* 8152 (Aug. 31, 2022), available at: *https://crsreports.congress.gov/product/pdf/LSB/LSB10776.*

22. *See* Joseph Duball, *Calif. Privacy Agency Takes Aim at Dismantling Federal Privacy Preemption*, Int'l Ass'n of Privacy Prof'ls (July 29, 2022), *https://iapp.org/news/a/cppa-takes-aim-at-dismantling-american-data-privacy-and-protection-acts-preemption/.*

23. Preemption clause of ADPPA, § 404(b).

24. Danielle Keats Citron & Alison Gocke, *Nancy Pelosi Is Blocking Landmark Data Privacy Legislation—for a Good Reason*, Slate (Sept. 9, 2022, 5:50 a.m.), *https://slate.com/technology/2022/09/nancy-pelosi-data-priavcy-law-adppa.html*.

25. "Becoming GDPR compliant may require a year's worth of work, depending on the company's resources." Bartnick, *supra* note 18.

26. *See, e.g., Data Privacy*, American Land Title Ass'n, *https://www.alta.org/advocacy/data-privacy.cfm* (providing information on compliance plans in the context of real estate title examinations) (last visited Dec. 24, 2022).

27. Notes taken at Session 3, "Data Privacy 2021," by Elizabeth Blosser of American Land Title Association, during the 2021 Annual Convention of the Louisiana Land Title Association on Dec. 1, 2021, in New Orleans, Louisiana (on file with author).

Jeff D. McAlpin is a 2017 graduate of Southern University Law Center with admissions to the Alaska (2017) and Louisiana (2019) bars. He has taught advanced legal analysis and writing at SULC since 2020 and is a solo practitioner based in St. Tammany Parish. (jeff.d.mcalpin@gmail.com; www.mcalpinlawfirm.com)