AN A.S. PRATT PUBLICATION
APRIL 2019
VOL. 5 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 | NUMBER 3 | APRIL 2019

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:
Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call
Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [69] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Momentum Builds for a National Privacy Law in the United States

Gregory P. Luib*

Although many contentious issues will need to be resolved, indications are that Congress will give serious consideration to a federal privacy law in this Congressional session. The author of this article discusses the proposals on the horizon and issues that will need to be resolved.

Recent developments show that momentum is building for the United States to enact a national privacy law that would govern how businesses handle consumers' personal information. High-profile data breaches, recent Congressional hearings and a Trump Administration privacy proposal have resulted in an unprecedented level of interest in federal privacy legislation. Although many contentious issues will need to be resolved, indications are that Congress will give serious consideration to a federal privacy law in this Congressional session.

DEVELOPMENTS DRIVING INTEREST IN A NATIONAL PRIVACY LAW

Among the impetuses for a federal privacy law are the recurring reports of suspected data breaches and misuses of consumer data. Such events have impacted companies in a wide variety of industries, including social media, health insurance, credit reporting, and travel and leisure. New data privacy laws in Europe and California are also driving stakeholders to pursue a national privacy law. In May of this year, the General Data Protection Regulation, or GDPR, went into effect in the European Union, introducing extensive data security obligations for companies handling sensitive information collected from European citizens. A month later, closer to home, the California Consumer Privacy Act was signed into law. Although the Act will not go into effect until 2020, it is arguably the most far-reaching data protection law ever enacted in the United States.

Multiple Congressional hearings this fall focused on the current state of consumer data privacy and possible approaches to safeguarding privacy more effectively. At one of those hearings, several large technology and communications companies voiced support for a national privacy law (in some form), based on concerns about the patchwork of state laws that currently exists, global interoperability of privacy policies

* Gregory P. Luib is counsel at Dechert LLP focusing his practice on antitrust and competition matters. Resident in the firm's Washington, D.C., office, he may be contacted at gregory.luib@dechert.com.

to ensure cross-border data flows, and the United States' ability to influence international privacy policy discussions.[1]

NOTABLE RECENT PRIVACY PROPOSALS

Against this backdrop, several national privacy frameworks recently have been proposed by the Trump Administration, individual members of Congress, and various stakeholders. These proposals have taken different approaches to core issues such as the inclusion of a baseline privacy standard, public and private enforcement mechanisms, and federal preemption of state laws.

Trump Administration Proposal

In September, the National Telecommunications and Information Administration ("NTIA") proposed and sought comments on a national approach to consumer privacy. As NTIA explained,

> The time is ripe to provide the leadership needed to ensure that the United States remains at the forefront of enabling innovation with strong privacy protections. . . . The Administration hopes to articulate a renewed vision, one that reduces fragmentation nationally and increases harmonization and interoperability nationally and globally.[2]

NTIA stated that it was not necessarily calling for the creation of a statutory privacy standard. Rather, it identified the following privacy outcomes that should be produced by any federal privacy framework that may be enacted:

- Transparency of privacy policies;
- Reasonable control by users of their data;
- Reasonable minimization of the data collected and used by organizations;
- Data security;
- User access to, and ability to correct, their data;
- Management/mitigation of the risk of harmful uses or exposure of personal data; and
- Accountability of organizations collecting and using data.

NTIA further issued a set of high-level goals that any national privacy framework should pursue, including:

---

[1] *See, Examining Safeguards for Consumer Data Privacy*, Hearing Before S. Comm. on Commerce, Sci. & Transp., 115th Cong. (2018), at https://www.commerce.senate.gov/public/index.cfm/hearings?ID=2FF829A8-2172-44B8-BAF8-5E2062418F31.

[2] Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600 (Sept. 26, 2018), *available at* https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy.

- Harmonize the regulatory landscape, which currently involves "a patchwork of competing and contradictory baseline laws";
- Legal clarity while maintaining the flexibility to innovate;
- Comprehensive application (*i.e.* a framework that applies to all private sector organizations that collect, store, use, or share personal data in activities not covered by sectoral laws, such as HIPAA);
- Employ a risk- and outcome-based approach, rather than "a compliance model that creates cumbersome red tape";
- Interoperability with international frameworks and norms;
- Incentivize privacy research;
- Federal Trade Commission ("FTC") as the federal agency to enforce consumer privacy (with certain exceptions for sectoral laws outside the FTC's jurisdiction); and
- Scalability (i.e. different approaches for small businesses that collect little personal information, distinctions between organizations controlling and those merely processing data).

More than 200 organizations and individuals filed comments on the NTIA's proposed framework, with many commenters submitting their own detailed privacy proposals.[3]

Federal Trade Commission Proposal

In comments filed with the NTIA, FTC staff expressed its support for "a balanced approach to privacy that weighs the risks of data misuse with the benefits of data to innovation and competition."[4] Perhaps unsurprisingly, the comment touted the FTC's unique ability to enforce any federal privacy framework, based on the agency's risk-based approach, dual consumer protection-competition jurisdiction, experience with privacy-related rulemaking, and institutional expertise.

Interestingly, the FTC staff comment noted that the agency has brought cases under various statutes addressing at least four types of privacy-related harms, including:

- Financial injury (e.g., identity theft, fraudulent charges, delayed benefits);
- Physical injury (e.g., risks from stalking or harassment);
- Reputational injury; and
- Unwanted intrusion (e.g., intrusions on the sanctity of one's home, unwanted telemarketing, and spam).

[3] The comments filed with the NTIA are available at https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy.

[4] FTC Staff, Comments Filed in Response to NTIA, Developing the Administration's Approach to Consumer Privacy, at 8 (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/federal_trade_commission_staff_comment_to_ntia_11.9.2018.pdf.

At a Congressional oversight hearing at the end of November 2018, FTC Chairman Joseph Simons identified the following additional tools the agency needs to protect consumer privacy: (1) rulemaking authority; (2) jurisdiction over nonprofits and common carriers; and (3) authority to impose civil penalties for first-time offenses (rather than just violations of existing orders). At that hearing, a majority of the FTC Commissioners voiced their support for seeking monetary penalties for data and privacy violations.

Congressional Proposals

Several data privacy bills have been introduced in the current session of Congress. However, on November 1, Senator Ron Wyden of Oregon released a discussion draft of one of the most far-reaching privacy bills to date, explaining:

> It's time for some sunshine on this shadowy network of information sharing. My bill creates radical transparency for consumers, gives them new tools to control their information and backs it up with tough rules with real teeth to punish companies that abuse Americans' most private information.[5]

Wyden's draft bill consolidates privacy enforcement with the FTC, empowering the agency, among other things, to:

- Issue regulations establishing minimum privacy and cybersecurity standards;
- Impose financial penalties up to four percent of a company's revenues for violations of such standards;
- Require CEOs, chief privacy officers, and chief information security officers of companies of a certain size to file with the FTC annual data protection reports that certify the companies' compliance with the privacy and cybersecurity standards; and
- Impose substantial fines and prison terms for any company officer who knowingly or intentionally certifies a false data protection report.

More recently, on December 12, Senator Brian Schatz of Hawaii and 14 other Democratic Senators introduced the Data Care Act, which would impose duties of care, loyalty, and confidentiality on online companies using personal data. In announcing the proposed legislation, Senator Schatz explained, "Just as doctors and lawyers are

[5] Press Release, U.S. Senator Ron Wyden, Wyden Releases Discussion Draft of Legislation to Provide Real Protections for Americans' Privacy (Nov. 1, 2018), *available at* https://www.wyden.senate.gov/news/press-releases/wyden-releases-discussion-draft-of-legislation-to-provide-real-protections-for-americans-privacy.

expected to protect and responsibly use the personal data they hold, online companies should be required to do the same."[6]

Key features of the Data Care Act include:

- *Duty of Care*: Companies must reasonably secure individual identifying data and promptly inform users of data breaches involving sensitive information (*e.g.*, social security or driver's license number, unique biometric data, children's information);
- *Duty of Loyalty*: Companies may not use individual identifying data in ways that will result in reasonably foreseeable and material financial or physical harm;
- *Duty of Confidentiality*: Companies must ensure that the duties of care and loyalty extend to third parties when disclosing, selling, or sharing individual identifying data;
- *Federal Enforcement*: A violation of the duties will be treated as a violation of the FTC Act and subject to monetary penalties, while the FTC is granted rule-making authority to implement the Act;
- *State Enforcement*: State attorneys general may enforce the Act, but the FTC can intervene and supersede state actions; and
- No federal preemption of state data and privacy laws.

Proposals Issued by Companies and Other Stakeholders

Intel recently released a draft federal privacy bill "to spur discussion on personal data privacy."[7] Key features of the bill include:

- Limitation on the use of personal information to purposes for which the consumer provides explicit consent, uses that are consistent with the original purpose, and as required by law or regulation;
- Required data security safeguards that are appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's activities, and the sensitivity of any personal data that is processed;
- Rulemaking authority for the FTC to issue privacy and data security regulations;
- Authority for the FTC to impose civil penalties up to $16,500 per individual for whom the covered entity unlawfully processed information, with an aggregate limit of $1 billion per violation;

[6] Press Release, U.S. Senator Brian Schatz, Schatz Leads Group of 15 Senators in Introducing New Bill to Help Protect People's Personal Data Online (Dec. 12, 2018), *available at* https://www.schatz.senate.gov/press-releases/schatz-leads-group-of-15-senators-in-introducing-new-bill-to-help-protect-peoples-personal-data-online?peek=SiLftL3PnsqT3q%2F0x2LCkfDVv5J0wufijMa%2BoVtnRqhaz6Mp.

[7] Press Release, Intel Corp., Intel Drafts Model Legislation to Spur Data Privacy Discussion (Nov. 8, 2018), *available at* https://www.businesswire.com/news/home/20181108005261/en/Intel-Drafts-Model-Legislation-Spur-Data-Privacy.

- Safe harbor for companies that certify that they are in compliance with the act; and
- Federal preemption of state privacy and data security laws.

The U.S. Chamber of Commerce ("Chamber") recently announced its support for a national privacy framework. After previously advocating for self-regulation in the privacy area, the Chamber has concluded that "today's current technological and state regulatory environment necessitates a federal privacy law that preempts state and local privacy laws."[8] The Chamber has released a set of privacy principles for policymakers that includes, among others:

- Congress should adopt a federal privacy framework that preempts state law on matters concerning data privacy, including breach notifications;
- Privacy protections should be risk-focused and based on the sensitivity of the data;
- The framework should be applied across all industry sectors;
- The framework should be flexible and not include mandates to use specific technological solutions;
- Enforcement should be limited to situations involving concrete harm to individuals; and
- Enforcement should not include a private right of action.[9]

In contrast, a group of consumer and privacy organizations – including, among others, the Consumer Federation of America, the Electronic Privacy Information Center, and the Center for Digital Democracy – recently released a draft framework for federal data protection that would include more enforcement measures and greater transparency than the proposals by Intel, the Chamber, and other private entities.[10] The key provisions of the draft framework include:

- No federal preemption of state privacy and data protection laws;
- A broad definition of "personal data" that includes information that identifies, or could identify, a particular person;
- Transparency of algorithmic and other automated decision-making to promote fairness and remove bias;
- Statutory damages for privacy violations;

---

[8] U.S. Chamber of Commerce, Comments Filed in Response to NTIA, Developing the Administration's Approach to Consumer Privacy, at 3 (Nov. 9, 2018), *available at* https://www.ntia.doc.gov/files/ntia/publications/u.s._chamber_ntia_privacy_comments_final.pdf.

[9] U.S. Chamber of Commerce, *U.S. Chamber Privacy Principles* (Sept. 6, 2018) *available at* https://www.uschamber.com/sites/default/files/9.6.18_us_chamber_-_ctec_privacy_principles.pdf.

[10] *Draft Framework for Data Protections in the United States from Consumer and Privacy Organizations* (Fall 2018), *available at* https://epic.org/testimony/congress/CPOs_to_SCC_US_Data_Protection_Framework_Oct2018.pdf.

- Private rights of action;
- Independent enforcement authority for state attorneys general; and
- Creation of a federal data protection agency (other than the FTC).

SIGNIFICANT ISSUES FOR THE NEXT CONGRESS TO RESOLVE

The proposals discussed above are just a sample of the numerous frameworks and guiding principles that governmental, private, and non-profit entities have proposed recently. As the Congress takes up national privacy legislation, as expected, it will need to sort through a host of issues on which there is likely to be strong disagreement among the various stakeholders. Based on recent proposals, those issues likely will include:

Privacy Standard and Other Threshold Issues

- Should organizations use self-regulation to achieve particular privacy outcomes, or should Congress enact a baseline privacy standard?
- Should the privacy law include specific measures and/or technologies that organizations must employ, or should the law be technology-neutral?
- Should Congress codify a specific privacy standard, or should it task the FTC or other federal agency to develop privacy regulations?
- Should the law include a safe harbor that identifies specific requirements for an organization to be considered in compliance?

Definition and Use of Personal Information

- How should Congress define the personal information that is subject to the privacy law? Should it be defined as broadly as in the GDPR (*i.e.* any information relating to an identified or identifiable natural person)?
- For which types of information, if any, should express consent be required?
- How should consent be defined? Opt-in, or opt-out?
- Should there be any prohibitions, limitations, or additional requirements imposed on the use of certain highly sensitive information (such as financial, health, children's, and precise geolocation data)?

User Control of Data

- How much control should users have over the data they have provided to organizations subject to the law?
- Should individuals have a "right to be forgotten" – or at least the ability to update and/or correct their information?
- Should individuals be able to "port" their data from one organization to another?

Federal Preemption of State Laws

- Should any federal law preempt state and local laws and regulations governing privacy and data security?

Coverage of the Law

- Should the law apply in the same manner to all companies with consumer data? That is, should the law be sector-neutral?
- Should the law replace or complement existing sector-specific federal laws, such as HIPAA or Gramm-Leach-Bliley?
- Should the obligations imposed by the law scale with the size of the organization, to reduce the compliance burden on smaller entities?
- Should the law address algorithmic or artificial intelligence-driven uses of consumer data?

Privacy Harms Addressed

- What types of privacy harms should the law seek to address: purely financial harms or a broader set of harms that includes reputational, emotional, and other more subjective forms of consumer harm?

Role of Federal Agencies

- Should the FTC enforce the law?
  - If so, should the FTC be granted additional authority, such as rulemaking authority to enact privacy and data security regulations? Or should it continue to use its existing authority to police unfair or deceptive conduct?
  - If not, should the law establish a new federal data protection authority (comparable to what many European nations currently have)?
- Will the Federal Communications Commission or any other sectoral regulator have a role in enforcing the privacy law?

Role of State Attorneys General

- Should state attorneys general be given concurrent authority to enforce the law (regardless of which entity serves as the federal enforcer)?

Penalties for Violations

- Should the law allow for the imposition of fines on organizations that violate the law?
- Should penalties include jail time for executives at organizations that violate the law?

Private Right of Action

- Should there be a private right of action to enforce the law?

Data Breach Reporting

- Should the law include a requirement for organizations to report data breaches?
- If so, how quickly and under what circumstances should the breaches be reported?

International Interoperability

- Should the law be designed to ensure interoperability with existing foreign privacy frameworks, such as the GDPR?

KEY TAKEAWAYS

- There is an unprecedented level of interest in and support for a national privacy law.
- The next Congress is likely to give serious consideration to a federal privacy law and could enact such a law in 2019.
- There will be substantial debate and disagreement over key aspects of any federal privacy law.
- Companies that handle consumer data should continue to regularly review their privacy and data security policies and practices to ensure that they are in compliance with existing laws and regulations, including both state privacy laws and the GDPR.
- Companies handling consumer data should consider the potential changes to their privacy and data security policies and practices that may be necessary if federal legislation is enacted.