Legal Backgrounder

Vol. 34 No. 15 September 27, 2019

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

The Case for Uniform Standards Grows as States Sew More Laws into Patchwork of Data-Privacy Regulations

by Boyd Garriott, Megan Brown, and Wes Weeks

Businesses in the United States face a patchwork of different state privacy and data security laws—a patchwork that is only expected to grow in the coming years. These laws differ state by state and often include vague requirements, such as demanding "reasonable" cybersecurity controls. With this multiplicity of state laws comes the specter of significant damages, stemming from statutorily granted private rights of action to sue. This collection of uncertain and—often—excessively punitive state laws can be a nightmare for businesses with little clear benefit to consumers. Luckily, this status quo is not set in stone. Federal preemption—either via a comprehensive federal privacy law or through the courts—could solve these problems and encourage a uniform national approach to an inherently interstate digital economy.

The State Privacy Landscape Is Complex and Is Worsening

While federal policymakers and agencies consider privacy regulation, states are taking action—and not necessarily in ways that are good for business. Take, for example, data breach laws. Every state, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have data breach notification laws.[1] Jurisdictions impose a wide variety of requirements. For example, in New York, post-breach disclosure requires (1) the contact information for the business and (2) a description of information that was improperly obtained.[2] Happen to also operate in Wyoming? There, a business must disclose:

- a description of the information that was improperly obtained;
- a general description of the breach;
- the approximate date of the breach;
- the general actions taken to protect from further breaches;
- advice to consumers to remain vigilant by checking their finances;
- whether the notification was delayed as a result of law enforcement investigation; and
- a toll-free number from which consumers can obtain the toll-free numbers and addresses of credit-reporting agencies.

It's not just the *content* of the breach notification that varies across state lines. States have different triggers for when a notification is even required. In Colorado, businesses must notify consumers if a student ID number is released with a first initial and last name.[3] Other state laws are triggered instead by release of biometric identifiers, mother's maiden name, or date of birth.[4] Some states require businesses to notify the state

[1] *See* Security Bread Notification Laws, Nat'l Conf. of State Legis., Sept. 29, 2018.
[2] However, New York recently amended its data breach law, effective October 2019.
[3] Colorado Revised Statutes, § 6-1-716.
[4] *See*, *e.g.*, Iowa Code Chapter 715C; North Dakota Code Chapter 51-30.

Boyd Garriott is an Associate, **Megan Brown** is a Partner, and **Wes Weeks** is an Associate, with Wiley Rein LLP in Washington, DC.

attorney general, others the state's consumer protection agency. Still others require businesses to notify credit-reporting agencies—some within a specific number of days (or hours) and others "without unreasonable delay." For organizations operating in multiple states, this patchwork is vexing. Compliance with varied statutes imposes serious burdens and costs on organizations that handle data.

In addition to data breach laws, states are enacting new privacy statutes. The 2018 California Consumer Privacy Act ("CCPA") grants a number of privacy "rights" to consumers, including the right to request that a business delete personal information about the consumer (with numerous exceptions) and the right to direct a business to not sell consumer information to a third party.[5] Some businesses are subject to additional obligations, like maintaining "a clear and conspicuous link" on the business's homepage to facilitate these rights.

Not all state privacy laws are as broad as the CCPA. Maine passed a privacy bill that prohibits Internet Service Providers from using, selling, or distributing subscribers' data without their "express, affirmative consent."[6] In May of this year Nevada passed a law that requires operators of Internet websites or online services that collect personally identifiable information ("PII") to comply with requests by consumers to not sell their data.[7] Vermont enacted a comprehensive "data broker" law last year that requires data brokers to register with the state Attorney General, file annual reports about their practices, and develop an information security program.[8]

Additional legislation is pending that would continue to restructure the privacy landscape of the United States. S. 120 in Massachusetts would, like the CCPA, give consumers multiple new privacy rights, including the right to have personal information deleted. It would also require businesses that collect personal information to notify consumers of what information it is collecting, why it is collecting the information, consumers' substantive rights granted by the statute, and more. Significantly, the law would create a private right of action for consumers against businesses with liquidated damages of up to $750 "per consumer per incident" and without the need to show any "loss of money or property." S. 224 in New York would similarly create new substantive consumer privacy rights and a private right of action for violations of the law.

Two states have passed Internet of Things ("IoT") security laws, opening up another area for divergent state regulation. Oregon and California require manufacturers of IoT devices to equip connected devices with "reasonable security features."[9] However, there are notable distinctions between the laws. The definition of "connected device" is broader in California: California regulates "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address," whereas Oregon focuses on devices that are "used primarily for personal, family or household purposes." As others have noted, "the Oregon law applies to *fewer* devices and to a *narrower* set of manufacturers . . ."[10] Such differences will become more pronounced if additional states pass IoT security laws, imposing technical mandates on manufacturers of devices that are created, sold, and managed across state lines.

These Laws Impose Real Costs on Businesses and Innovators, Large and Small

These laws drive up costs, imposing a drag on economic actors who shift resources to compliance. Complying with this assortment of diverse state laws imposes real and significant costs on the private sector, including small business and the innovation base. In preparation for the European Union's General Data Protection Regulation ("GDPR"), American Fortune 500 companies spent a combined $7.8 *billion*.[11] And while Fortune 500 companies might have multi-billion-dollar resources to foot the compliance bill, smaller companies will have a significantly

[5] California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798.100-1798.199. The state legislature has passed several amendments to the CCPA which, when this publication went to press, were awaiting the Governor's signature. These amendments make several changes to the law, including creating a time-limited exemption for employee data and certain business-to-business communications and transactions. The substantive provisions of the law, however, remain largely unchanged.

[6] An Act to Protect the Privacy of Online Customer Information (LD 946, to be codified at 35-A M.R.S. c. 94).

[7] An Act Relating to Internet Privacy, SB-220.

[8] Vermont Data Broker Regulation, Act 171 of 2018.

[9] *See* An Act Relating to Security Measures Required for Devices that Connect to the Internet (HB2395, amending ORS 646.607); SB-327 Information privacy: connected devices.

[10] Wiley Rein LLP News & Insights, *States Continue to Move Forward on Their Own Privacy and Security Laws: Nevada, Maine, and Oregon Are The Latest*, July 2019.

[11] O. Smith, *The GDPR Racket: Who's Making Money from this $9bn Business Shakedown*, FORBES, May 2, 2018.

tougher time. Indeed, earlier this year, a report from the Connected Commerce Council found that nearly *half* of all businesses agreed with the statement: "At this stage, the business wouldn't have the resources to cope with significant changes to data privacy regulations."[12]

These laws create operational inefficiencies and distort interstate markets for data, products, and services. The burdens of varied regulations go far beyond out of pocket expenses for new policies and legal bills. Businesses are evaluating and changing multi-state operations to account for shifting state obligations, resulting in the export of California's legal preferences across the country. This can affect how companies collect, store, and use data, and affect the architecture of their information systems and networks. It also affects organizations' consumer disclosures and websites, which may have to become more complex to address varied state rules. State inconsistency in regulating IoT products or technology like biometrics and facial recognition can also impact product and service design, as well as the marketing, sale, and use of technology, products, and services.

Litigation risk will drive up costs and chill innovation. In addition to enormous compliance costs and the distortion of interstate production, distribution, and marketing, several states are choosing to expose companies to significant legal liability—even where they have taken precautions to protect consumer data. For example, Illinois' Biometric Information Privacy Act ("BIPA") requires businesses to comply with several "procedural" requirements, such as obtaining written consent before collecting biometric identifiers and publishing a schedule for destroying biometric information.[13] BIPA also provides a private right of action—with damages ranging from $1,000 to $5,000 per violation—without any showing of *actual harm*.

The risk from this sort of statute is substantial. Just last month, in *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019), the Ninth Circuit held that plaintiffs could bring a class action against Facebook over the social network's use of "Tag Suggestions," a feature where Facebook uses facial recognition technology to suggest users to "tag" in photographs uploaded to the website. The Ninth Circuit determined that the suit was appropriate even where the plaintiffs were not harmed, had the opportunity to opt out, and the lead plaintiff admitted that he thought Tag Suggestions was a "nice feature." As the authors wrote at the time: "There are hundreds of pending BIPA suits. Facebook is looking at thousands of dollars in liquidated damages *per violation*. Sitting at just over 2 billion users, that can add up fast."[14] These astronomical damages appear to be here to stay. With the go-ahead by the Ninth Circuit, BIPA suits are likely to proliferate at an even faster rate. Moreover, both Massachusetts' S. 120 and New York's S. 224—if passed in their current form—would allow for private rights of action without requiring a showing of harm. These regimes create significant risks for businesses of all sizes—even if they are doing a great job at protecting consumers.

Congress or the Supreme Court Could Address this Problem.

Two entities could significantly alleviate the patchwork problem: Congress and the courts.

First, Congress could solve this problem by passing an expressly preemptive federal privacy law. Article VI, Paragraph 2 of the U.S. Constitution provides that the "Laws of the United States" are "the supreme Law of the Land." Known as the Supremacy Clause, this provision grants Congress the authority to preempt state laws. Congress could use this authority to pass a comprehensive privacy law that would preempt the patchwork of state laws described above. In so doing, it could give businesses a single standard with which to comply—instead of 50—and therefore ensure more consistent compliance with evolving privacy standards.

While Congress is actively working on federal privacy legislation, it remains to be seen whether that work will materialize into a bill. Moreover, some in Congress are opposed to preemption, arguing that it could water down privacy protections. Opposition to preemption is driven in part by a concern that government enforcement is inadequate, but also by attorneys and others who benefit from large settlements and damages awards. The legal system is no stranger to abusive litigation over "injury-free" technical violations that offer a reward of statutory damages, as the U.S. Chamber's Institute for Legal Reform has shown in research papers on the Telephone Consumer Protection Act and privacy class actions.[15]

---

[12] Small Business Data Regulation and Responsibility, Feb. 2019 at 45.

[13] 740 Ill. Comp. Stat. 14/1 *et seq*. (2008).

[14] B. Garriott, M. Brown, and W. Weeks, *Ninth Circuit Opens the Floodgates to Privacy Litigation*, Wiley Connect, Aug. 9, 2019.

[15] *See* TCPA Litigation Sprawl: A Study of the Sources and Targets of Recent TCPA Lawsuits, Aug. 2017; Ill-Suited: Private Rights of

ISBN 1056 3059

Second, federal courts could find that state privacy and cybersecurity requirements violate the Dormant Commerce Clause. The Dormant Commerce Clause prohibits states from imposing substantial burdens on interstate commerce because such burdens undermine the policy of free trade between the states articulated by the Constitution's grant of authority to Congress to regulate interstate commerce. The Internet is the quintessential "instrumentality of commerce" and should not lightly be regulated by states.[16]

Most of the digital economy is interstate and the interstate movement and use of data and technology facilitate additional interstate commerce. According to the United States Department of Commerce's Bureau of Economic Analysis,[17] "the digital economy" is made up of "three major types of goods and services":

- the digital-enabling infrastructure needed for an interconnected computer network to exist and operate;
- the e-commerce transactions that take place using that system; and
- digital media, which is the content that digital economy users create and access.

State privacy and security laws affect each of these categories.

The Supreme Court has held that laws regulating out-of-state activity or that substantially burden interstate commerce can be unconstitutional. For example, in *Bibb v. Navajo Freight Lines, Inc.*, 359 U.S. 520 (1959), the Court struck down an Illinois statute that required certain mudguards on trucks and trailers on Illinois highways. Finding the statute conflicted with other state regulations and would have severely disrupted trucking operations through Illinois, the Court held that the law "place[d] an unconstitutional burden on interstate commerce."

Here, courts could find that state privacy laws substantially burden interstate commerce and are unconstitutional under the Dormant Commerce Clause. Consider, for example, the Nevada law described above that requires website operators to establish a way for consumers to request that the website operator not sell their data. The law applies to any website operator that (1) collects and maintains PII from Nevada residents; and (2) "[p]urposefully direct[] its activities toward" Nevada. This law will subject most public-facing websites that engage in any kind of nationwide commerce to comply with the statute's procedural requirements. Regulating Internet communications and commerce targets a channel that is at least as fundamental to our system of interstate commerce now as the interstate highway system was when the Supreme Court decided *Bibb.* Likewise, regulation of the handling and use of data that is collected, moved, used, and stored across jurisdictional lines targets the lifeblood of the Internet economy.

Conclusion

The status quo is challenging and likely to worsen for organizations trying to comply with a shifting array of obligations. Companies face exploding compliance costs and may have to adjust interstate operations, manufacturing, marketing, and distribution of their products and services. Nationwide markets may be effectively regulated by one or a few states.

Worse, the specter of ever-growing statutory damages from lawsuits exploiting this patchwork of state privacy and security laws looms large. Things are likely to get worse if states are left unchecked. States—including New York, with its population of nearly 20 million—are contemplating far-reaching privacy laws with private rights of action.

Immeasurable dead-weight losses to the economy can be avoided, however. The most direct course of action would be for Congress to pass preemptive federal privacy and data security legislation. Congress can clarify the primacy of federal superintendence over the inherently interstate digital economy. In doing so, Congress should recognize the mistake it made with statutory damages in the TCPA and reject calls for enforcement of privacy and data security through private litigation. However, Congress need not be the only actor. Regulated entities can and should present courts with the opportunity to protect the interstate digital economy from disruptive and burdensome state privacy laws that unconstitutionally burden interstate commerce.

Action and Privacy Claims, July 2019.

[16] *See* Instrumentalities and Channels of Interstate Commerce, 29 CFR § 776.29.

[17] K. Barefoot, *et al.*, *Defining and Measuring the Digital Economy*, Bureau of Economic Analysis Working Paper, Mar. 15, 2018.

  ISBN 1056 3059