Divergent State Privacy Laws Show Need For Federal Solution

By **Seamus Duffy, Meredith Slawe and Julie Busta** (July 9, 2019)

Seamus Duffy

Meredith Slawe

Julie Busta

As we approach the effective date of the California Consumer Privacy Act in 2020, businesses nationwide are scrambling to ready themselves for a patchwork of new state privacy laws. The CCPA has been the principal focus for many, to be sure, but a new Nevada law targeting sales of consumer personally identifying information harvested from online activity will actually become effective before the CCPA (Oct. 1 of this year).

Other states have enacted and are considering laws that will cascade into effect in the coming few years. None of these laws tracks the CCPA perfectly, and each law will present its own operational challenges for businesses navigating the digital marketplace.

Meanwhile, a U.S. Senate working group is considering a federal solution that might preempt the patchwork of state laws and offer much-needed clarity and uniformity. It has been widely reported that this group, composed of Sens. Roger Wicker, R-Miss., Richard Blumenthal, D-Conn., Maria Cantwell, D-Wash., Brian Shatz, D-Hawaii, John Thune, R-S.D. and Jerry Moran R-Kan., hopes to present a bill before the Senate recess in August.

Here's hoping the working group acts, because, if there is no thoughtful and comprehensive federal solution with broad preemption, an already complex web of laws will likely continue to evolve at the state level and pose significant challenges to businesses with multistate and national footprints. Consider just a few of the first states that have had bills percolating through the legislative process.

An Emerging Patchwork of Disparate State Laws

Nevada is targeting cookies and web tracking alone.[1] It will be the first state to provide consumers the right to opt out of the sale of their personal information. Unlike the now-famous "Do Not Sell My Personal Information" homepage button required by the CCPA, the Nevada law requires a more conventional email address, toll free number or website for opt-out requests.

Nevada has its own set of required disclosures for its residents that differ from the CCPA transparency regime. The definitions of "consumer" and "personal information," core elements of any privacy law, are different from those set forth in the current version of the CCPA.

So, for the 608-mile border that California and Nevada share, we will have a magic website button and robust rights of access and deletion on just one side, and a web-tracking statute with an entirely different scope of protected information on the other. A Nevada resident who works across the border in California will not enjoy the rights of access and deletion the CCPA provides to her co-workers but will enjoy a special set of rights over web tracking activity when she returns home.

New York's proposed law, if passed, will be landing directly in the epicenter of the digital marketplace. The New York Privacy Act tracks most of the core elements of the CCPA, creating rights of access, portability and deletion of its own with deadlines for fulfilling data subject requests that differ from that of the CCPA.[2]

Most importantly, the NYPA would introduce the concept of the "data fiduciary" to the quilt. Inspired by an idea offered a few years ago by law professors Jack Balkin of Yale University and Jonathan Zittrain of Harvard University, the New York law would pronounce data controllers "fiduciaries" to data subjects. As fiduciaries, data controllers subject to the statute would owe duties of "care, loyalty and confidentiality" which would require the data controller to "act in the best interests of the consumer, without regard to the interests of the [controller]."

The text of the bill as proposed states boldly "[t]he fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity." In a lively hearing before the New York Senate consumer affairs and protection committee on June 4, 2019, representatives of the business community emphasized the disruption to the tech sector such a concept could produce. The New York law, unlike the CCPA, applies to all businesses — large and small — and in its current form includes a robust private right of action.

Maine's new law, broadly titled An Act to Protect the Privacy of Online Consumer Information, oddly singles out internet service providers alone.[3] The Maine law, based loosely on a set of Federal Communications Commission rules adopted under President Barack Obama and later repealed before they ever became effective by a Republican-controlled Congress that accompanied President Trump into office, would subject ISPs to a data privacy regime that would apply to no other businesses in Maine.

Signed into law by Gov. Janet Mills on June 6, 2019, the law is set to take effect in July 2020 if it survives the inevitable challenges in the courts. Unlike the other emerging state laws, this law targets a very specific segment of the telecommunications market — a segment already heavily regulated by the FCC. Importantly, it seeks to undo prior federal Congressional action.

The new law working its way through the legislative process in neighboring Massachusetts, An Act Relative to Consumer Data Privacy, may be the broadest yet and the most dangerous from a risk-management standpoint.[4] Tracking the CCPA rights of access, deletion, portability and nondiscrimination, the Massachusetts law takes the CCPA revenue threshold down to $10 million and broadens the definition of protected information, particularly biometric information.[5]

Most importantly, the Massachusetts law provides a private right of action and $750 in statutory damages per violation, with no damages cap and no requirement of actual injury. The statute prohibits any contractual waiver of its terms and declares unlawful and unenforceable any limitation on a consumer's "remedies or means of enforcement."

Meanwhile in neighboring Vermont, the Legislature last year decided to target only data brokers. Act 171 of 2018 imposes registration requirements on data brokers, who are required to report annually on their practices and any data breaches they suffer or have suffered.[6] The Vermont law does not require consent or permit Vermonters to opt out of data sales but requires brokers to disclose in their reports whether they provide consumers the right to opt out.

The law provides special rights to Vermonters to order "credit freezes" from credit reporting agencies free of charge to protect their credit reports in the event of a data breach. It imposes requirements for maintaining the security of protected data. Violation of the law constitutes an unfair trade practice under Vermont's general consumer protection statute.

Colorado has taken a different approach, focusing exclusively on data security. An Act Concerning Strengthening Protections for Consumer Data Privacy, became law last September.[7] With a far more traditional definition of "personal identifying information" (name, address, social security number, passport number, student ID, etc.),[8] this law requires covered entities to maintain "reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations."

The Colorado law requires adoption of written procedures for disposal of both electronic and paper form PII when the information is no longer needed, and sets forth very specific notice and related requirements for data breach response. The Colorado statute highlights and exacerbates the difficulties companies have encountered in developing compliance strategies for the plethora of state laws governing data breaches.

A Call for a Comprehensive Federal Solution

The CCPA contains an interesting "poison pill" provision not often found in groundbreaking state legislation. This provision voids the statute if, and to the extent, it is "preempted by, or in conflict with, federal law."[9] The provision is unnecessary, of course, because the supremaclause of the U.S. Constitution accomplishes the purpose.

Some have read this provision as a signal by the drafters of the CCPA that a federal solution would be preferable, even by them. Put another way, this provision of the statute suggests that the CCPA's authors may have intended their efforts to spur the federal government to more decisive action on data privacy.

If Congress fails to enact a preemptive law addressing data privacy issues, and we instead opt for the states to act as legislative laboratories for a period of years as some have suggested, we will pay a very high price. The Internet has been likened to air transport or radio communications — it cries out for a uniform national regulatory scheme. We cannot chop up the Internet into 50 separate data privacy territories, each with special rules for data security, access, deletion and transparency.

This is why the nations of the EU adopted the General Data Protection Regulation to provide a uniform set of principles for the EU digital economy. If this revolution in data privacy rights is to occur in America, as seems apparent, we need one reasonable definition of personal information — not 50 competing ones.

Interstate businesses cannot possibly track individual states' particular sets of rules for defining, securing, processing, accessing and deleting data. Nor can we expect companies to maintain separate home pages for each state with different disclosures, links and buttons relating to data privacy.

As the initial wave of more general state data privacy laws demonstrates, data privacy laws are complex, and they call for important policy trade-offs and balances. If some states target particular market participants for special regulation, as Maine and Nevada have, that will unfairly prejudice those companies in a very competitive marketplace.

A checkerboard of different enforcement regimes, some with robust private rights of action like New York and Massachusetts and others based on the single regulator model like the CCPA, will plague the courts with difficult venue and choice of law problems as enterprising lawyers exploit the vagaries of these new statutes. The class action bar will flock to the states with friendly enforcement regimes and push the limits of these new laws, disrupting efforts by businesses expending their resources developing sound compliance strategies.

Perhaps most importantly, the overall costs of compliance will soar if companies are required to develop separate compliance plans for each state, without any indication that the costs will result in improved protections for consumers.

Seamus Duffy and Meredith Slawe are partners and Julie Busta is an associate at Akin Gump Strauss Hauer & Feld LLP.

[1] S. 220, 80th Sess. (Nev. 2019), https://www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6365/Text.

[2] S. 5642, Reg. Sess. (N.Y. 2019), https://legislation.nysenate.gov/pdf/bills/2019/S5642.

[3] S. 946, 129th Sess. (Me. 2019), http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=SP0275&item=1&snum=129.

[4] S. 120, 191st Sess. (Mass. 2019), https://malegislature.gov/Bills/191/S120.pdf.

[5] The proposed law defines "biometric information" as including "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information." S. 120 § 1(b). https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdfThis definition goes beyond Illinois' definition in its Biometric Information Privacy Act ("BIPA"), passed in 2008. The BIPA has been the source of a significant wave of litigation, and has presented difficult jurisdictional and venue puzzles for the courts.

[6] H. 764, G.A. (Vt. 2018), https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.

[7] Colo. Rev. Stat. § 6-1-713 (2018), https://leg.colorado.gov/sites/default/files/2018a_1128_signed.pdf.

[8] The definition of PII also includes "biometric data," which is defined rather restrictively as "unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account." Colo. Rev. Stat. § 6-1-716(1)(a). Thus, while the proposed Massachusetts law broadens the scope of protected biometric information beyond the definition in Illinois statute that has led the way, the Colorado law would restrict it.

[9] Cal. Civ. Code § 1798.196 ("This title is intended to supplement federal and state law, if permissible, but shall not apply if such application is preempted by, or in conflict with, federal law or the United States or California Constitution.").