Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 32, ISSUE 26 / JUNE 5, 2015

EXPERT ANALYSIS

Fixing the Patchwork: Will Congress Enact A Federal Data Breach Law?

By Christopher J. Cox, Esq., David R. Singh, Esq., and John Stratford, Esq.
Weil, Gotshal & Manges

The past year has seen a multitude of high-profile data breaches dominating the news and the number of reported security breaches continuing to rise.[1] As more consumers find themselves on the receiving end of breach notification letters from health care providers, banks, restaurants and retailers, more attention has focused on the legal framework governing companies' obligations to provide breach notifications — and, specifically, its failings.

As President Barack Obama succinctly stated in January, "Right now, almost every state has a different law on this, and it's confusing for consumers and it's confusing for companies — and it's costly, too, to have to comply [with] this patchwork of laws."[2]

In one sense, the much-maligned patchwork of 47 different state breach notification laws, aimed at protecting consumers and holding companies accountable in an environment where personal information is increasingly exposed, has been successful because it has forced companies to publicize the occurrence of data breaches, thus increasing awareness of data security among businesses and consumers.[3]

Still, companies understandably bemoan the inherent conflicts and complexities presented when attempting to meet their reporting obligations. Has the time finally come for the federal government to respond to the calls for an overarching federal statute? Or will states continue to lead the way?

This commentary considers that question by briefly revisiting the statutory framework governing data breach notification in the United States and reviewing some of the latest legislative developments in state and federal law.

STATE DATA BREACH NOTIFICATION LAWS

To date, 47 states — all but Alabama, New Mexico and South Dakota — have enacted data breach notification laws.[4]

California, a recognized leader in data privacy legislation, enacted the first breach notification law in 2003, and most state notification laws follow its general structure. The statutes generally require businesses to notify affected individuals of an unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality or integrity of personal information held by the business.

The California statute defines "personal information" as an individual's first name or initial with last name in combination with sensitive information such as a Social Security number, financial account information, or medical or health insurance information.[5]

While the general thrust of each state's law is the same, there is significant and widely noted variation among the state laws, which has given rise to the so-called patchwork problem. For example, a majority of states require notification only if the breach poses, or is likely to pose, a significant risk of harm to the affected individuals.[6] Other states, such as California, include no such requirement.

The differences do not stop there — some states have expanded the traditional definition of "personal information" to include biometric or DNA data, tribal identification numbers, and email account information.[7] Some states require notification to the state attorney general, law enforcement or consumer protection agencies,[8] and, particularly concerning to businesses, a minority of states allow individuals to sue for damages.[9]

One of the most widely cited points of divergence among state data breach laws is the timing of notification. Under California's law, for example, businesses must notify individuals of any breach of unencrypted personal data "in the most expedient time possible and without unreasonable delay." But other states impose specific timeframes. For example, Florida requires notification within 30 days after discovery of the breach, and Ohio, Wisconsin and Vermont require notification within 45 days.[10]

Notably, various combinations of state laws can lead to strange results and conflicting obligations. Massachusetts, for example, provides that a notice of security breach "shall not include the nature of the breach or unauthorized acquisition or use of the number of residents of the commonwealth affected by said breach or unauthorized access or use,"[11] while other statutes expressly require at least a general description of the breach.[12]

As a result of these and other variations, the "patchwork" has garnered widespread reproach from companies and commentators alike.[13]

Still, the state law framework continues to evolve.

Has the time finally come for the federal government to respond to the calls for an overarching federal statute? Or will states continue to lead the way?

In the aftermath of recent large-scale breaches, states have rushed to tighten existing requirements. Legislators in Target's home state of Minnesota, for instance, proposed an (eventually unsuccessful) amendment that would have required businesses to provide notice within 48 hours after discovery of a security breach and to reimburse customers for any fraudulent expenses incurred as a result of a breach. Florida successfully shortened its notification period from 45 days to 30 days. In New York the attorney general is backing legislation that would broaden the definition of personal information under the state's data breach notification statute.[14]

The most recent state law amendments are slated to take effect later this year. Wyoming expanded its definition of personal information; Montana did the same and added a new requirement for notification to the office of its attorney general; and, on April 23, Washington amended its statute to cover noncomputerized data, require attorney general notification and set a 45 day time limit on notification.[15]

FEDERAL LEGISLATIVE PROPOSALS

This frenzy of activity in state legislatures further explains why calls for a uniform federal data breach law have only increased.

In addition to extending federal protection to consumers in the three states with no breach notification laws, a federal breach notification statute would give national businesses a uniform set of rules to follow, making compliance easier and less expensive.

Despite these advantages, attempts at enacting federal legislation have been controversial, particularly with respect to the issue of federal preemption of state law. While preemption would seem to solve the patchwork problem, the idea has met strong opposition from some state and consumer advocates.

State attorneys general, who are often empowered by state data breach notification laws, have resisted legislation that would restrict their enforcement powers.[16] And privacy advocates have objected to federal standards that would preempt more stringent state laws that require quicker notification or provide for a private right of action.[17]

It is unsurprising, then, that recent proposals for a federal data breach notification law that would have preempted state law have failed. In the U.S. Senate, for example, bills proposed by Democrats Patrick Leahy of Vermont, West Virginia's Jay Rockefeller (now retired) and Richard

Blumenthal of Connecticut would have preempted state data breach notification laws while granting enforcement authority to state attorneys general.

A bill by Pennsylvania Republican Pat Toomey would have gone a step further to preempt not only data breach notification laws but also any law pertaining to the security of personal data. Meanwhile, a bill by Democrat Tom Carper of Delaware would have preempted all state action, including any law intended to protect the security of consumer data, safeguard data from misuse or mitigate the harm resulting from security breaches.

Likewise, in the early months of 2015, Carper and Leahy have introduced new data breach bills, as have Florida Democrat Bill Nelson and Missouri Republican Roy Blunt, while Senator Democrat Mark Warner of Virginia suggested that he is preparing to make his own offering.[18] To date, none of these bills has been reported out of committee.

THE WHITE HOUSE PROPOSAL

A recent proposal from the executive branch is illustrative of the potential terms of — and pitfalls inherent in — these federal data breach proposals.

On Jan. 13 President Obama announced a proposal for federal data breach legislation that largely drew upon previous legislative proposals and indeed has much in common with subsequent bills introduced this year in Congress.

Under the White House proposal, business entities that store "sensitive personally identifiable information" of more than 10,000 individuals would be required to provide notification of security breaches without "unreasonable delay," defined as fewer than 30 days.[19] Businesses would be able to delay notice to affected individuals if they were able to prove that additional time was "reasonably necessary" to assess the scope of the breach or prevent additional disclosures.

Forty-seven states — all but Alabama, New Mexico and South Dakota — have enacted data breach notification laws.

In addition to providing notice to affected consumers, business entities would be required to provide notice to an agency to be designated by the secretary of the U.S. Department of Homeland Security when more than 5,000 individuals are affected by any particular breach.

The proposal would also provide several exemptions to the notice requirement. Under the national security and law enforcement exemption, no notice would be required if the Secret Service or FBI determines that notification might "reveal sensitive sources" or if the FBI determines that providing notice "could be expected to cause damage to national security." Under the safe-harbor provision, a business would be exempt from providing notice if it conducts a risk assessment — the results of which must be submitted to the Federal Trade Commission — and determines there is "no reasonable risk that a security breach has resulted in, or will result in, harm to affected individuals."

Finally, under the financial fraud prevention exemption, a business would be exempt if it uses a security program that "effectively blocks the use of sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual."

The 30-day notification requirement has been criticized because it imposes a stricter time frame than most state statutes and because it would limit the amount of time available for businesses to investigate a breach.

The proposal also includes a state law preemption provision that would be of particular importance to businesses that engage in interstate commerce.

As currently formulated, the proposed statute would supersede any state law "relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data." The law would also grant state attorneys general authority to bring suit to enjoin any practice that does not comply with federal requirements, to enforce compliance and to impose penalties of up to $1,000 per day per violation.

There is significant and widely noted variation among the state laws, which has given rise to the so-called patchwork problem.

However, the preemption provision has already been the subject of much debate. Indeed, at a January hearing held by the Commerce, Manufacturing, and Trade Subcommittee of the House Committee on Energy and Commerce to discuss the elements of a federal data breach statute, the question of federal preemption was a central point of disagreement.[20]

Although the White House proposal may provide a template for a future federal statute, and while it shares many provisions with other proposals currently in Congress, the contours of the notification requirement and the extent to which federal legislation would preempt state data breach notification laws remain unclear. No consensus has been reached and varying federal proposals continue to be introduced.[21]

As FBI Director James Comey quipped, large companies in the United States can be divided into two categories: those that have been hacked, and those that don't yet know they have been hacked.[22] Whether or not one's outlook is as dire as Comey's, one thing is clear: Between rapidly evolving state laws and unprecedented political will focused on a federal data breach notification standard, it is imperative for businesses that operate across state lines to stay abreast of the frequent state patchwork changes until a federal standard finally emerges.

NOTES

[1] Verizon's 2015 Data Breach Investigations Report observed that The New York Times published more than 700 articles related to data breaches in 2014, versus fewer than 125 the previous year. *See* Verizon Enter. Solutions, *2015 Data Breach Investigations Report* (2015), http://vz.to/1K2pCSp; *see also* Privacy Rights Clearinghouse, Chronology of Data Breaches, http://bit.ly/1PXffky (last visited May 20, 2015). The Privacy Rights Clearinghouse reported almost 300 data security breaches in 2014, comprising over 67 million individual records.

[2] *See* David Hudson, *The President Announces New Actions to Protect Americans' Privacy and Identity,* The White House Blog (Jan. 12, 2015, 6:01 PM), http://1.usa.gov/1Hv5rin.

See, e.g., 5-42 David Bender, *Computer Law: A Guide to Cyberlaw and Data Privacy Law,* § 42.03 (Matthew Bender, Rev. Ed. 2015)..

[4] *Security Breach Notification Laws,* Nat'l Conference of State Legislatures (Jan. 12, 2015), http://bit.ly/1EGwuFg.

[5] Cal. Civ. Code § 1798.82(h).

[6] *See, e.g.,* Conn. Gen. Stat. § 36a-701b (providing that notification is not required if an investigation "determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed").

[7] *See, e.g.,* Iowa Code Ann. § 715C.1; N.C. Gen. Stat Ann. § 75-61; Wyo. Stat. Ann. § 40-12-501; Cal. Civ. Code § 1798.82(h)(2).

[8] *See, e.g.,* Cal. Civ. Code § 1798.82(f); Wis. Stat. Ann. § 134.98(2); Haw. Rev. Stat. § 487N-2(f); N.Y. Gen. Bus. Law § 899-aa(8).

[9] *See, e.g.,* Cal. Civ. Code § 1798.84; Wash. Rev. Code § 19.255.010(10); Va. Code Ann. § 18.2-186.6.

[10] Cal. Civ. Code § 1798.82(a); Fla. Stat. § 501.171(4)(a); Ohio Rev. Code § 1349.19; Wis. Stat. § 134.98; Vt. Stat. tit. 9, § 2435.

[11] Mass. Gen. Laws § 93H, § 3(b).

[12] *See, e.g.,* Vt. Stat. tit 9, § 2435.

[13] *See, e.g.,* David Ruiz, *Patchwork of State Laws Adds to Data-Breach Headaches,* The Recorder (Apr. 10, 2015), http://bit.ly/1PXhu7m.

[14] *See* H.F. 2253, 88th Leg. (Minn. 2014); Fla. Stat. § 817.5681 (repealed 2014); Fla. Sta. § 501.171(4)(a) (2014); Press Release, Office of Attorney General Eric T. Schneiderman, *A.G. Schneiderman Proposes Bill to Strengthen Data Security Laws, Protect Consumers from Growing Threat of Data Breaches* (Jan. 15, 2015), http://bit.ly/1Hv8LKg.

[15] Wyo. S.F. 36 (effective July 1, 2015), *available at* http://bit.ly/1PNk6K7; Mont. H.B. 74 (effective Oct. 1, 2015), *available at* http://1.usa.gov/1JVmCt3; Wash. H.B. 1078 (effective July 31, 2015), *available at* http://1.usa.gov/1HLkW5X.

[16] *See, e.g.,* Protecting Consumer Information: Can Data Breaches Be Prevented? Hearing Before the H. Subcomm. on Commerce, Manufacturing, and Trade Committee on Energy & Commerce, 113th Cong. (2014) (statement of Lisa Madigan, Attorney General of Illinois), *available at* http://1.usa.gov/1GDxpqT.

[17] *See, e.g.,* Ctr. for Democracy and Tech., Letter to Chairman John Thune and Ranking Member Bill Nelson re: Data Breach Legislative Proposals (Feb. 5, 2015), http://bit.ly/1PXiyYW.

[18] Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014) (as proposed by Sen. Patrick Leahy); Data Security and Breach Notification Act of 2014, S. 1976, 113th Cong. (2014) (as proposed by Sen. Jay Rockefeller); Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014) (as proposed by Sen. Richard Blumenthal); Data Security and Breach Notification Act of 2013, S. 1193, 113th Cong. § 6 (2014) (as proposed by Sen. Pat Toomey); Data Security Act of 2014, S. 1927, 133th Cong. § 7 (2014) (as proposed by Sen. Tom Carper); Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. (2015) (as proposed by Sen. Bill Nelson); Data Security Act of 2015, S. 961, 114th Cong. (2015) (as proposed by Carper and Sen. Roy Blunt); *see* Consumer Privacy Protection Act of 2015, 114th Cong. (2015), *available at* http://1.usa.gov/1Bp7RHW (as proposed by Leahy); *see* Cory Bennett, *Dem preps Senate's third data breach bill,* The Hill (Apr. 27, 2015, 11:45 AM), http://bit.ly/1cOYtao.

[19] Personal Data Notification & Protection Act § 101(c) (2014) (as proposed by President Obama).

[20] *See* What Are the Elements of Sound Data Breach Legislation? Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Energy and Commerce Comm., 114th Cong. (Jan. 27, 2015).

[21] *See* Consumer Privacy Protection Act of 2015, 114th Cong. (2015), *available at* http://1.usa.gov/1Bp7RHW; *see also* Eric Chabrow, *Another Breach Notification Bill Introduced,* Bank Info Security (Apr. 30, 2015), http://bit.ly/1LcfTsZ.

[22] *See* James Cook, *FBI Director: China Has Hacked Every Big US Company,* Bus. Insider (Oct. 6, 2014, 6:24 AM), http://read.bi/1BcJrkK.



Christopher J. Cox (L), a partner with **Weil, Gotshal & Manges** in Silicon Valley, leads the firm's California complex commercial litigation practice and is a member of the cybersecurity, data privacy and information management group. He can be reached at chris.cox@weil.com. **David R. Singh** (C), also based in Weil's Silicon Valley office, is counsel in the firm's litigation department and a member of its complex commercial litigation practice and cybersecurity, data privacy and information management group. He can be reached at david.singh@weil.com. **John Stratford** (R) is an associate in the firm's Silicon Valley office, where he focuses on complex commercial litigation. He can be reached at john.stratford@weil.com.