Bloomberg BNA

Privacy and Security Law Report®

Data Breach Notification

Companies will be left in a legal quagmire of inconsistent state data breach notification requirements unless Congress repairs the broken system by passing legislation to replace the patchwork of state laws, the authors write, as they analyze proposals for implementing a unified federal standard.

The Need to Repair the Complex, Cumbersome, Costly Data Breach Notification Maze



By Mark L. Krotoski, Lucy Wang, and Jennifer S. Rosen

Mark L. Krotoski is a litigation partner in the Privacy and Cybersecurity and Antitrust practices of Morgan, Lewis & Bockius LLP in Silicon Valley and Washington. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.

Lucy Wang is an associate in the Litigation practice of Morgan, Lewis & Bockius in San Francisco.

Jennifer S. Rosen is an associate in the Litigation practice of Morgan, Lewis & Bockius in San Francisco.

I. Introduction

Companies face many cyber-threats from several sources today. Significant data breaches can result from organized, international hacking groups; state-sponsored actors; hackers for hire; cyber terrorists; hacktivists; an insider threat; and even employee inadvertence or misconduct. The perpetrators seek information of value ranging from social security numbers, health information, credit card numbers and confidential company information to trade secrets. Much of the time, however, the data breach is a result of cybercrime.

After a breach, a number of data breach notifications are triggered for customers and also enforcement agencies. In fact, navigating the notification requirements can become a cumbersome nightmare. The failure to do so properly can result in lawsuits and enforcement actions.

 ISSN 1538-3423

Consider a common recent data breach example: Sophisticated cyber-thieves launch a spearfishing e-mail attack against a target company. Despite cyber-trainings and policies, the company discovers that an employee's e-mail account was compromised.[1] Consequently, the criminals penetrated the company's security systems, accessed and stole confidential information.

Upon discovery, the company immediately launched an investigation to determine the cause and scope of the breach. For example, did the hackers access personally identifiable information (PII), protected health information (PHI), payment card information (PCI), trade secrets or other confidential information? Moreover, were any customers impacted and what if any information was exfiltrated or used? The answers may take weeks to determine. The full scope of the breach may not be known for several months.

After being the victim of a cybercrime, however, the company must also confront a maze of disclosure obligations. The customer notification requirements will depend on the customer's residence and jurisdiction of enforcement agencies. Almost every state has data breach notification requirements, but they can differ significantly in their scope and application. In California and Florida, for example, a customer's user name and security question would qualify as protected information. Not so in Wisconsin or Connecticut. State laws differ not only in the types of data breaches they regulate, but also in who, what, when and how they require companies to notify their customers. In California, Florida and Connecticut, for example, companies may also be required to notify particular state agencies. Hence, even though the company operates nationally and its security systems are managed centrally, the company must tailor each notification to fit the specific requirements of the state in which each customer resides.

The variations between each state's laws create a complex and burdensome system for companies operating across many jurisdictions.

Failure to do so exposes the company to state penalties for technical non-compliance as well as potential civil litigation. Depending on the type of information (*e.g.*, PII, PHI, PCI or trade secrets), companies may be subject to multiple overlapping federal and state regimes. For example, reporting may be required to the Securities and Exchange Commission (SEC),[2] Dep't of Health and Human Serv. (HHS),[3] Federal Communication Commission (FCC),[4] and other federal and state agencies. Again, some states, including California and Wisconsin, exempt companies from their data notification laws if the subject information is separately regulated under a the Health Insurance Portability and Accountability Act (HIPAA). Other states, such as Florida and Connecticut, have no such exemption.

Consider, for example, the issue of ''who'' must be notified. Data breach standards differ on whether the customer or individual must be notified every time there is a breach. Some states—such as Connecticut, Florida, and Wisconsin[5]—have a harm analysis that is used to determine whether notification is required, while others—such as California[6]—do not.

In addition to notifying the individual, some state laws require a public report filing but differ on the circumstances when the report must be filed. Illustratively, California and Florida require a report when the PII was disclosed for more than 500 residents.[7] When notice is given to more than 1,000 persons, other states require notice such as Hawaii which requires notification to the Office of Consumer Protection,[8] Missouri requiring notice to ''the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis,''[9] and North Carolina similarly requiring notice to ''the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.''[10] Massachusetts requires notification of the breach to the ''to the attorney general, the director of consumer affairs and business regulation and to such [affected] resident.''[11] Under these different state statutes, the same breach incident can result in mandated disclosures to individuals and public agencies in some jurisdictions but not others. With state data breach notification laws becoming increasingly complex and often conflicting, the objective of assisting consumers has become unnecessarily complex, costly and cumbersome. The question now is whether this multitude of state laws is creating more confusion than clarity and undermining the original objectives for data breach notification? The notification process should not be this challenging for compliance.

This article analyzes the development of state notification laws and current proposals for implementing a unified federal standard. For the reasons discussed below, policymakers should act to simply the notification requirements so they remain meaningful.

[1] The example draws upon the recent ''Business E-mail Compromise'' which has adversely impacted many financial services and other companies. *See, e.g.*, U.S. Dep't of Justice, Fed. Bureau of Investigation, Fin. Serv. Info. Sharing and Analysis Ctr. and U.S. Secret Serv., *Fraud Alert—Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses* (June 19, 2015), http://src.bna.com/cge.

[2] *See, e.g.*, Div. of Corp. Fin., Sec. and Exch. Comm'n, CF Disclosure Guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

[3] *See, e.g.*, HIPAA Breach Notification Rule, 45 CFR § § 164.400-414; *see also* Notice to the Sec'y of HHS, Breach of Unsecured Protected Health Information.

[4] *See, e.g.*, 47 C.FR 64.2011 (Notification of customer proprietary network information security breaches); *see also* Customer Proprietary Network Information (CPNI) Breach Reporting Facility.

[5] *See* Conn. Gen Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.

[6] *See* Cal. Civ. Code § § 1798.29(*), 1798.80(*).

[7] Cal. Civ. Code § § 1798.29(e), 1798.80(f); Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i).

[8] Haw. Rev. Stat § § 487N-2(f).

[9] Mo. Rev Stat. § 407.1500.2(8).

[10] N.C. Gen. Stat. § § 75-61, 75-65(f).

[11] Mass. Gen. Laws § 93H-1.3(b).

  PVLR ISSN 1538-3423

II. Proliferating State Data Breach Notification Laws

In 2002, California enacted the first data security breach notification law, which became effective in July 2003.[12] The objective of this new law was to allow consumers to protect themselves against identity theft and mitigate damages resulting from unauthorized access to their information.[13] In a little more than a decade, the state data breach standards have proliferated. Today, 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have adopted data breach notification laws.[14]

Broadly speaking, most data breach notification laws follow the basic tenets of California's original law. In each jurisdiction, lawmakers passed laws requiring entities to notify individuals when there is a reasonable belief of unauthorized acquisition of or access to data that compromises the security, confidentiality or integrity of an individual's covered personal information.[15] Responding to a data breach under any of these laws, however, is a multi-step process—a company must (1) ascertain if a breach has occurred; (2) determine whether the data at issue (typically PII) triggers data breach notification in one or more of the 51 applicable jurisdictions (in addition to any federal notification requirements); (3) determine who to notify (such as customers and public agencies); and (4) determine what, when, and how to notify them.[16]

a. Conflicts Between State Notification Laws.

Based on the proliferation of data breach notification standards, compliance with data breach notification laws can be complicated in any one jurisdiction, and the variations between each state's laws create a complex and burdensome system for companies operating across many jurisdictions. Companies operating in each of the 51 jurisdictions must, for example, must identify and reconcile the differences between requirements such as the timing of the notification. While some state's notification laws require quicker notification than others', in practice, multi-jurisdictional companies must determine, and uniformly follow, the most rigorous applicable standard in order to streamline the process. This requires familiarity with each of the differing notification windows, some of which are defined vaguely as the ''most expedient time possible,''[17] and others which range from as few as 30 days,[18] to as many as 90 days.[19]

Once a business has identified the shortest applicable notification period, it must wade through the many other differences between data breach notification laws. Most immediately, it is necessary to determine what kind of PII is covered under the applicable states' laws. While most states' definitions of PII cover similar ground—social security number, driver's license number, state ID card number and account or credit/debit card number along with an access code[20] —some states have expanded definitions of protected PII subject to the data breach notification laws, such as a user name/e-mail address and password[21], and an individual's DNA profile or unique biometric data (*e.g.*, fingerprint, voice print, retina or iris image).[22] Even where states' definitions of PII overlap, there are often nuanced distinctions that make a significant impact on an entity's notification obligations. For instance, some states protect only *electronic* data,[23] while others protect PII in any form.[24]

Making the discovery and notification process even more cumbersome, states' notification triggers vary from an unauthorized ''acquisition'' of PII,[25] to unauthorized ''access'' to PII,[26] and in some states either an unauthorized acquisition *or* unauthorized access can trigger the notification laws.[27] Moreover, some states provide exemptions from the notification laws where an entity has complied with separate laws. For example, some (but not all) states exempt entities that are covered by HIPAA and have complied with the notice requirements in Section 13402(f) of the Health Information Technology for Economic and Clinical Health Act (HITECH).[28]

A comparison of a few sample states' requirements further demonstrates the complicated maze of the state data breach notification laws:

b. Evolving New Standards and Moving Targets.

To complicate matters, because the laws in this area are constantly evolving, the most rigorous standards across each applicable jurisdiction are moving targets. For instance, in 2015, at least 32 states introduced or are considering, security breach notification bills or resolutions.[33] Among other things, these bills contemplate amending existing data breach notification laws to require entities to report breaches to the local attorney general or another central state agency; expand the definition of PII (*e.g.*, to include medical, insurance or biometric data); require businesses or government entities to implement security plans or various security measures; and require educational institutions to notify parents or government entities if a breach occurs.[34] California alone enacted several laws this year amending its data breach notification requirements.[35] Among other things, the new laws include data collected through the use of an automated license plate recogni-

[12] S.B. 1386 (Cal. 2002) (amending Cal. Civ. Code § § 1798.29, 1798.82).
[13] *Id.* at § 1.
[14] *See* Nat'l Conference of State Legislatures (NCSL), Security Breach Notification Laws (listing jurisdictions).
[15] *See, e.g.*, Conn. Gen Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.
[16] *Id.*
[17] *See, e.g.*, Cal. Civ. Code § 1798.29(a).
[18] *See, e.g.*, Fla. Stat. § 501.171(4)(a).
[19] *See, e.g.*, S.B. 949 (Conn. 2015) (*amending* Conn. Gen. Stat. § 36a-701b).
[20] *See, e.g.*, Cal. Civ. Code § § 1798.29, 1798.82; Conn. Gen. Stat. § 36a-701b; Fla. Stat. § § 501.171, 282.0041, 282.318(2)(i); Wis. Stat. § 134.98.
[21] *See, e.g.*, Cal. Civ. Code § 1798.29(g)(2); Fla. Stat. § 501.171(g).
[22] *See, e.g.*,Wis. Stat. § 134.98(1)(b).
[23] *See, e.g.*, Cal. Civ. Code § 1798.29(a); Fla. Stat. § 501.171(1)(a); Conn. Gen. Stat. § 36a-701b(a).
[24] *See, e.g.*, Wis. Stat. § 134.98.
[25] *See, e.g.*, Cal. Civ. Code § 1798.29(f); Wis. Stat. § 134.98.
[26] *See, e.g.*, Fla. Stat. § 501.171(1)(a).
[27] *See, e.g.*, Conn. Gen. Stat. § 36a-701b(a).
[28] *See, e.g.*, Cal. Civ. Code § 1798.81.5(e)(3); Wis. Stat. § 134.98(3m)(b).
[33] NCSL, 2015 Security Breach Legislation.
[34] *Id.*
[35] *Id.*

Data Breach Notification Maze

California[1]	Florida[2]	Wisconsin[3]	Connecticut[4]
Definition of Personally Identifying Information (PII)			
(1) An individual's first name or first initial and last name in combination with: • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card / debit card number in connection with any code permitting access to an individual's financial account; • Medical information; • Health insurance information Or (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account.	(1) An individual's first name or first initial and last name in combination with: • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card/debit card number in connection with any code permitting access to an individual's financial account; • Medical information; • Health insurance information • Passport number; • Military ID number; • Any other number issued on a government document used to verify identity; Or (2) User name or email address, in combination with a password or security question and answer that would permit access to an online account.	An individual's first and last name or first initial and last name in combination with: • Social Security Number; • Driver license number; • State ID card number; • Account number or credit card/debit card number in connection with any code permitting access to an individual's financial account; • DNA profile; • Unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.	An individual's first name or first initial and last name in combination with: • Social Security Number; • Driver license number; • State ID card number • Account number or credit/debit card number with any required code permitting access to an individual's financial account.
Notification Trigger			
When an Entity discovers or is notified of an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of PII maintained by the Entity.	When an Entity knows, or reasonably believes, there has been unauthorized access to PII in electronic form.	When an Entity discovers or is notified that PII in the Entity's possession has been acquired by a person whom the Entity has not authorized to acquire the PII.	When an Entity knows, or reasonably believes, there has been unauthorized access to or acquisition of electronic files, media, databases, or computerized data containing PII.
Timing of Notification			
The most expedient time possible without unreasonable delay.	30 days	45 days	90 days
Attorney General to be Notified?			
Yes (if an Entity is required to notify more than 500 CA residents).	Yes (if an Entity is required to notify more than 500 individuals in FL).	No.	Yes.

[1] Cal. Civ. Code §§ 1798.29, 1798.80 et seq.
[2] Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i).
[3] Wis. Stat. § 134.98.
[4] Conn. Gen Stat. § 36a-701b.

A BNA Graphic/data29g1

PVLR ISSN 1538-3423

Data Breach Notification Maze

California[1]	Florida[2]	Wisconsin[3]	Connecticut[4]
Manner of Notification			
The notice shall disclose any breach of the security of the system following discovery or notification of the breach. Notice may be provided by: • Mail; or • Electronically, provided it is consistent with 15 U.S.C. § 7001 (E-SIGN Act). • The notice shall be written in plain language and shall include (among other things) a description of: • The date of the notice; • Name and contact information of the Entity; • Type of PII subject to the unauthorized access and acquisition; • The date, estimated date, or date range during which the breach occurred; • Whether notification was delayed as a result of law enforcement investigation; • A general description of the breach incident; • The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.	**Attorney General** Written notice must include (among other things): • A synopsis of the events surrounding the breach • The number of individuals in Florida who were or have potentially been affected by the breach. • A copy of the notice required to affected individuals. **Affected Individuals** Notice must contain, at a minimum: • The date, estimated date, or estimated date range of the breach. • A description of the PII that was accessed or reasonably believed to have been accessed. • Information regarding how to contact the Entity to inquire about the breach. Notice may be provided by: • Mail; or • E-mail.	The notice shall indicate that the Entity knows of the unauthorized acquisition of PII. Notice may be provided by: • Mail; or • A method the Entity has previously employed to communicate with the subject of the PII.	The notice shall disclose any breach of security following the discovery of the breach. Notice may be provided by: • Mail; • Telephone; or • Electronically, provided it is consistent with 15 U.S.C. § 7001 (E-SIGN Act). • Additionally, Entities must offer and disclose identity theft prevention services and, if applicable, identity theft mitigation services, at no cost for up to one year.
Risk of Harm Exemption			
No.	Yes—notice to affected individuals is not required if the Entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to those whose PII has been accessed.	Yes—an Entity is not required to provide notice of the acquisition of PII if the acquisition of PII does not create a material risk of identity theft or fraud to the subject of the PII.	Yes—notification is not required if the Entity reasonably determines that the breach will not likely result in harm to those whose PII has been acquired and accessed.
HIPPA Exception			
Yes.	No.	Yes.	No.

[1] Cal. Civ. Code §§ 1798.29, 1798.80 et seq.
[2] Fla. Stat. §§ 501.171, 282.0041, 282.318(2)(i).
[3] Wis. Stat. § 134.98.
[4] Conn. Gen Stat. § 36a-701b.

A BNA Graphic/data29g2

tion system within the scope of protected PII.[36] This marks the third set of amendments to California's notification laws within the last three years.[37]

c. The Effects of Disparate State Notification Laws.

The patchwork of state laws related to data security make corporate compliance with the notification laws both unnecessarily difficult and costly. Moreover, even after conducting a comprehensive investigation and response to the breach itself, there is still the risk that companies may face litigation for non-compliance with some technical requirements of each state's notification laws. According to a study conducted by the Ponemon Institute in May 2015, the average cost of a data breach to a U.S. company in 2015 was $6.5 million, which represents an 11% increase in the total cost of data breach since 2014.[38]

Such burdens and costs often do not result in the protections the laws are intended to provide. With such a confusing system of requirements, consumers are left without confidence in the safeguards protecting their personal information. According to a 2012 study by the Ponemon Institute, 72% of people who receive notification of a data breach were dissatisfied with the communication they received.[39]

The consequences of non-compliance can result in enforcement actions by state attorneys general or other agencies.[40] Additionally, some states (such as California, Hawaii and Louisiana) permit a private right of action to be brought for the failure to provide timely disclosure.[41]

III. Early Recognition on the Need for A Uniform Federal Standard

Within a couple of years of the first state laws going into effect, Congress was already considering multiple proposals for federal legislation. Indeed, the states themselves were calling for national leadership. In a letter to congressional leaders in 2005, Attorneys General from 48 states urged Congress to take action and create federal requirements for notifying consumers of data breaches. Attorneys General from states that had already passed notification laws as well as states without such laws agreed that consumers would benefit from a ''national security breach notification law.''[42] Moreover, while the Attorneys General recommended that federal preemption should be limited in scope, they acknowledged that federal law may govern the ''timing, manner and content of security breach notification laws.''[43]

In the decade that followed, every single Congress has considered—but failed to pass—a national security breach notification law. In that time, however, the need for federal legislation has only intensified. Not only have the instances of cyberattacks risen, but the proliferation of state notification laws have made it increasingly difficult for companies to deliver timely and consistent information to consumers.

IV. Competing National Standard Proposals

During his State of the Union Address, President Obama noted the importance of addressing cyber security issues and enacting legislation ''to better meet the evolving threat of cyber attacks, combat identity theft, and protect our children's information.''[44] One part of the Administration package included a Personal Data Notification & Protection Act.[45] If passed, the Personal Data Notification & Protection Act would replace the current patchwork of state laws with a unified national standard for notifying consumers when their personal information has been compromised.[46]

The Personal Data Notification & Protection Act, however, is only one of many proposals currently pending before Congress. Like the mosaic of state laws, each federal proposal takes a slightly different position on what constitutes personal information, what conditions trigger notification, what information must be disclosed, when the information must be disclosed, and what consequences should be imposed for non-compliance. In addition, the federal proposals also differ on whether (or to what extent) federal law should preempt overlapping state laws.

Among the competing proposals, one gained early traction—the Data Security and Breach Notification Act

---

[36] *Id.*

[37] LawFlash, California Amends its Breach Notification Requirements (AGAIN) (Nov. 19, 2015) (summarizing new California data breach requirements) (14 PVLR 1893, 10/19/15).

[38] Ponemon Institute, 2015 Cost of Data Breach Study: United States.

[39] Ponemon Institute, 2012 Consumer Study on Data Breach Notification.

[40] Many state data breach statute provide for state enforcement actions. *See, e.g.*, Ariz. Rev. Stat. § 44-7501H (''This section may only be enforced by the attorney general. The attorney general may bring an action to obtain actual damages for a wilful and knowing violation of this section and a civil penalty not to exceed ten thousand dollars per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.''); Kan. Stat. § 50-7a02(g) (''For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate.'').

[41] *See, e.g.*, Cal. Civ. Code § 1798.84(b) (''Any customer injured by a violation of this title may

institute a civil action to recover damages.''); Haw. Rev. Stat. § 487N-3(b) (''any business that violates any provision of this chapter shall be liable to the injured party in an amount equal to the sum of any actual damages sustained by the injured party as a result of the violation''); La. Rev. Stat. § § 51:3075 (''A civil action may be instituted to recover actual damages resulting from the failure to disclose in a timely manner to a person that there has been a breach of the security system resulting in the disclosure of a person's personal information.'').

[42] Testimony of Assistant Attorney General Julie Brill before Subcommittee on Financial Institutions and Consumer Credit Committee on Financial Services, U.S. House of Representatives (Nov. 9, 2005), enclosing Letter from Attorneys General to Congressional Leaders (Oct. 27, 2005; updated Nov. 7, 2005).

[43] *Id.*

[44] *Id.*

[45] The Personal Data Notification & Protection Act.

[46] The White House Office of the Press Secretary, Securing Cyberspace - Preside Obama Announces New Cybersecurity Legislative Proposal and other Cybersecurity Efforts (January 13, 2015).

  PVLR ISSN 1538-3423

(H.R. 1770).[47] Jointly authored by Representative Marsha Blackburn (R-Tenn.) and Representative Peter Welch (D-Vt.), the Data Security and Breach Notification Act focuses on the pressing concerns of identity theft and financial fraud in e-commerce. In that context, the act defines personal information to include social security numbers, financial and other account credentials (including biometric credentials) and names coupled with driver's license numbers.[48] Upon discovering a security breach impacting personal information, companies must conduct a good faith investigation and take necessary measures to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data system.[49] Once the company has done so, it must notify consumers of the breach within 30 days unless there is no reasonable risk of identity theft, economic loss, economic harm or financial fraud.[50]

States continue to enact new privacy laws and revise existing laws at an almost feverish pace, which may, individually, be in the best interest of each states' residents. Taken collectively, however, this mish-mash of constantly changing state law is making it increasingly difficult for companies keep consumers informed.

Under the legislation, companies may delay notification for law enforcement or national security purposes.[51] Otherwise, however, failure to notify constitutes an unfair and deceptive act or practice under the Federal Trade Commission Act.[52] Both the FTC and State Attorneys General have enforcement power to seek civil penalties from violators.[53]

Finally, consistent with the President's proposal, Data Security and Breach Notification Act would also create a unified national standard by preempting state notification laws.[54]

V. Opposition from State Attorneys General

Just as the Data Security and Breach Notification Act is gaining some momentum, however, State Attorneys General issued another letter, this time to block a national notification law. In a new letter to Congressional leaders this summer, Attorneys General from forty seven states joined in opposing any federal legislation that would preclude states from enacting different or more stringent requirements.[55] Attorneys General from several states—including California, Massachusetts and Illinois—have also spoken out individually, sometimes specifically to criticize the Data Security and Breach Notification Act.[56]

Among other things, the State Attorneys General argue that Data Security and Breach Notification Act and similar proposals undercut existing protections for consumers under state law.[57] Federal law, they argue, may set a national floor of protection. However, Congress should not prevent any State from enacting tougher laws within their borders nor restrict a State Attorney General's authority to pursue violators.

Echoing these concerns, a coalition of Democratic Senators and Representatives introduced a competing proposal—the Consumer Privacy Protection Act (S. 1158/H.R. 2977).[58] Unlike the Data Security and Breach Notification Act, the Consumer Privacy Protection Act only preempts state laws to the extent they contain ''less stringent'' requirements for notification.[59] Hence, the Consumer Privacy Protection Act allows State Attorneys General to continue enforcement actions under more restrictive state standards.

Federal preemption would not eliminate the role of state attorneys general. To the contrary, each of the federal legislative proposals contemplates that state attorneys generals will be able to bring enforcement actions for violations of the federal data breach notification law.

Meanwhile, the Data Security and Breach Notification Act itself has stalled. Although the bill passed through the House Energy and Commerce Committee in April, the vote was split along party lines: 29 (Republican) - 20 (Democrat).[60] Even the bill's original co-author, Democratic Representative Peter Welch, ultimately voted with other Democrats in opposing his own bill.[61]

[47] H.R. 1770, 114th Cong. 1st Sess. (2015).
[48] *Id.* § 5.10(A).
[49] *Id.* § 3(a).
[50] *Id.* § § 3(a)(3) & 3(c).
[51] *Id.* § 3(c).
[52] *Id.* § 4(a).
[53] *Id.* § § 4(a) & 4(b).
[54] *Id.* § 6(a).
[55] Letter from Attorneys General to Congressional Leaders (July 7, 2015).
[56] *See, e.g.*, Letter from California Attorney General Kamala D. Harris to Chairman and Ranking Member of House Committee on Energy and Commerce (May 4, 2015); Office of Massachusetts Attorney General Maura Healey, AG Healey Raises Concerns About Federal Bill That Would Weaken Data Breach Protections for Massachusetts Residents (March 18, 2015); Office of Illinois Attorney General Lisa Madigan, Madigan Testifies as Congress Considers Data Breach Notification Law (Feb. 5, 2015).
[57] Letter from Attorneys General to Congressional Leaders (July 7, 2015).
[58] S. 1158, 114th Cong., 1st Sess. (2015); H.R. 2977, 114th Cong., 1st Sess. (2015).
[59] *Id.* § 205.
[60] Energy & Commerce Committee, United States House of Representatives, Data Security Solution Moves Forward (April 15, 2015);
[61] Elise Viebeck, *Controversial Data Breach Bill Pass House Committee*, The Hill (April 15, 2015).

At this point, it remains uncertain whether Data Security and Breach Notification Act or any other proposal for federal legislation will gain sufficient support become law.

VI. Inconsistent Standards Persist

Against the congressional debate, States continue to enact new laws and revise existing laws at an almost feverish pace. Taken individually, each State may be acting in the best interest of its residents in trying to keep consumers informed. Taken collectively, however, this mish-mash of constantly changing state law is making it increasingly difficult for companies to do just that. Instead of providing greater protections for consumers, States are creating a legal quagmire that only ends up impeding companies' abilities to respond effectively to data breaches. Policymakers need to consider how consumers are served by the data breach notification confusion that persists under current law.

Some clarity needs to be restored to the data breach notification process. At this juncture, only Congress can do so.

Contrary to the positions taken by the State Attorneys General, federal law would not gut protections for consumers. To be sure, whichever legislative proposal is ultimately passed, it will likely be narrower than some existing state laws. However, federal law will cover jurisdictions that currently have no data breach notification laws and will also likely be broader than some existing state laws.

More importantly, federal law would create a uniform national standard that would benefit both consumers and companies. Consumers across the country would have a clearer understanding of what information is protected. Companies will also be better prepared to respond to a data breach. Instead of trying to comply with a multitude of sometimes conflicting laws—and risking sanctions for potential technical noncompliance—companies can instead devote their resources to quickly investigating and remedying the data breach.

Moreover, federal preemption would not eliminate the role of state attorneys general. To the contrary, each of the federal legislative proposals contemplates that state attorneys generals will be able to bring enforcement actions for violations of the federal data breach notification law. State attorneys general, therefore, would continue to be at the forefront of protecting their residents when cybercriminals attack.

At the end of the day, all stakeholders—federal and state, Democrats and Republicans, companies and consumers—have the same shared goal. If (and more likely when) a company is the target of cybercrime, we want the company to investigate the breach and inform consumers whose personal information has been compromised. A unified national standard would set clear and consistent expectations for what steps companies must take and what information consumers can expect to receive in the event of a data breach.

VII. Conclusion

The current data breach notification laws are no longer working effectively. The process has become unnecessarily complex, costly and cumbersome.

There is no consensus among the states to simply or improve the process. Consequently, only Congress can repair the system. Bi-partisan support is needed for federal legislation to replace the current patchwork of state laws governing data breach notification. Without federal action, companies will be left in this legal quagmire of inconsistent state notification requirements. The maze of state laws is making it increasingly difficult for companies to notify customers with clear and timely information. Congress should step in to improve data notification standards. One federal standard will best serve the needs of both companies and consumers.

  PVLR ISSN 1538-3423