

What's the Big Hurry?

The Urgency of Data Breach Notification

Ellen Cornelius, J.D. | Senior Law & Policy Analyst
University of Maryland Carey School of Law, Center for Health & Homeland Security



DATA BREACH NOTIFICATION

Globally, about 5 million data records are lost or stolen each day. For each theft, consumers spend an average of 20 hours and \$770 to attempt to rectify their losses. Individuals' reputations suffer, sometimes permanently. Consumers should take action after they are notified of a data breach because there is a good chance that criminals are already using or selling their data. Once personal data is made public, a Federal Trade Commission study showed that it is only minutes before the first unauthorized access attempt is made. Using a stolen social security number, criminals can generate new loans, new credit accounts, new medical debts, and fabricated tax returns.

Protecting personal information needs to be a priority, but companies need to be held accountable as well. For example, Equifax knew that there was a vulnerability and did not address it by installing an available patch. Millions of people were impacted by the Equifax data breach. As a result, eight states signed consent decrees with Equifax that required remedial actions, but did not include fines. This pattern has repeated many times. Breaches occur on a daily basis because safeguards are not in place or are not effective. Furthermore, existing laws do not provide adequate remedies that can be imposed by a well-defined authority. Something must change.

The patchwork of vague state laws is a consumer's sole recourse after a data breach. Personal

information is varying described as any combination of: first name, last name, social security number, driver's license number, account number, credit card number, debit card number, personal health care information, username, and password. The varied nature of state data breach laws means that there are numerous standards for notification as well. Once a data breach is discovered, vague language in state laws allows companies to delay notification to consumers. The laws employ words such as "as expeditiously as possible," "without unreasonable delay," or "as soon as possible." There is no uniform standard governing when companies must provide meaningful notification to consumers.

The fragmented nature of state laws could be tackled by federal legislation that sets a floor for notification, standardizes the definition of personally identifiable information (PII), and eliminates vague language. In order for a federal law to preempt state law, it must represent the exercise of a power conferred on Congress by the Constitution, and the legislation at issue must regulate private actors. Whatever legislation is passed must be crafted using express language and must regulate private actors rather than states.

Consumers need a comprehensive data breach law that preempts state law, especially one that requires notification within seventy-two hours.

Seventy-two hours is the optimum amount of time between the discovery of a breach and notification, and a seventy-two hour requirement would harmonize American law with European Union law.

Seventy-two hours is the optimum amount of time between the discovery of a breach and notification, and a seventy-two hour requirement would harmonize American law with European Union law. Two examples are instructive. In 2018, the European Union enacted the General Data Protection Regulation (GDPR), which requires seventy-two hour notification. After an entity becomes aware of a breach, it has seventy-two hours to notify the data protection authorities. Seventy-two hours gives a company enough time to prepare a response, but it also gives the consumer a chance to mitigate the harm that often results from data loss. Many breaches are undetected for months. By the time the consumer is notified, a significant amount of time may have lapsed. As exemplified by recent support for the California





Consumer Privacy Act, the public has deep concerns regarding privacy and transparency with respect to data collection. At present, California is considering SB 1121, which specifies that if a company is dilatory in protecting users' social security numbers or does not comply with the California notification requirements, users are entitled to seek monetary damages. Consumers would be able to "institute a civil action to recover damages" and consumers could seek up to \$1,000 "per customer, per incident or actual damages, whichever is greater."

The seventy-two hour standard should benefit consumers who are entitled to know whether their social security number, credit card number, password, or other personally identifiable information has been compromised. Sixty day notification is too long. Forty-five day notification is too long. Even fifteen days is too long. If consumers are notified within seventy-two hours, then they can monitor their accounts for small charges that are often test charges before large charges are made. They

can close checking accounts with associated debit cards because debit cards carry less protection than credit cards; they can set up fraud alerts; they can change passwords; they can use two-factor authentication; and, they can scrutinize emails for suspicious activity.

Federal legislation would increase protection for consumers and make compliance more streamlined for businesses. If Congress enacted a uniform standard to protect consumers, it could displace contrary law and make compliance easier for companies. Federal legislation could account for GDPR and state legislation. If Congress enacted a similar standard, consumers would be given the date of the breach and a description of what was stolen. This would require a company to improve its cyber compliance practices.

There are already efforts to pass federal legislation in Congress. Senator Bill Nelson introduced the Data Security and Breach Notification Act¹ to the committee on November 30, 2017. This bill

would require mandatory notification within thirty days of a data breach, carry a five year prison sentence for intentionally hiding a data breach, and provide financial incentives for companies using technologies which make consumer information unreadable in the event of a breach.

There was a congressional hearing in March 2018 on a draft bill that would serve as federal data breach legislation. The proposed legislation would preempt state laws; but, it would be similar to California, which, as discussed, has strict data breach legislation on the books. Equifax and other credit agencies would be excluded as well as banks and financial institutions; however, these entities are covered under the Gramm-Leach-Bliley Act (legislation that regulates financial institutions and customer information). The legislation includes a major loophole if a company determines that no reasonable risk of a data breach exists. Specifically, the legislation that Representatives Luetkemeyer and Maloney introduced states the following:

Individuals benefit when they are given the chance to act quickly to close bank accounts, set up fraud alerts, and change passwords.



**MASTER OF SCIENCE IN LAW
Cybersecurity Law**

**designed for today's
busy professionals!**

ONLINE | PART-TIME | AFFORDABLE

www.law.umaryland.edu/online

 UNIVERSITY
of MARYLAND
FRANCIS KING CAREY
SCHOOL OF LAW


If a covered entity determines after completion of the preliminary investigation under subsection (a) that there is a reasonable risk that the breach of data security has resulted in or will result in identity theft, fraud, or economic loss to any consumer, the covered entity shall immediately notify such consumer, without unreasonable delay except under circumstances outlined in paragraph (5), Sec. 4 (b)(2).

Finally, Senators Amy Klobuchar and John Kennedy introduced the Social Media Privacy and Consumer Rights Act² of 2018. Their legislation, similar to the GDPR, requires notification within seventy-two hours of a privacy violation. While these examples of legislation are a step forward, they are not the overhauls in the area of data breach law that are much needed.

Some state attorneys general and large trade groups argue against federal legislation requiring notification within seventy-two hours because preemption could render their statutes obsolete. States argue that the federal government will not enforce the laws, that the states can act faster than the federal government, and that the states have been leading the charge

thus far. Additionally, companies argue that they will be singled out and penalized. Some companies claim that companies need time to engage law enforcement and subject matter experts who work to identify the attackers. States may not want to yield this area of law to the federal government; however, the federal government has more resources. Data breaches can stretch state resources and cross state lines. Furthermore, state attorneys general trade groups could still enforce local laws by means of civil litigation.

Consumers want more, not less, protection. Individuals benefit when

they are given the chance to act quickly to close bank accounts, set up fraud alerts, and change passwords. As seen on a daily basis, comprehensive data breach legislation is needed. Consumers would benefit from having one definition of personally identifiable information, one data breach authority, and a seventy-two hour notification requirement. While states may argue that the federal government will not enforce the law, the state regulators will still have a part to play. And, while companies may argue that adopting the European Union's or California's consumer protections are too onerous, the resounding advantage is uniformity. 

About the Author



Ellen Cornelius received her J.D. from the University of Maryland in 2005 and is a member of the Maryland and District of Columbia bars. Since joining CHHS in 2008, Ms. Cornelius has worked for the District of Columbia's Homeland Security and Emergency Management Agency and Maryland's Department of Health and Mental Hygiene. Ms. Cornelius teaches three courses at the University of Maryland Francis King Carey School of Law: Law and Policy of Cybersecurity, Legal Ethics, and Legal Analysis and Writing.



Sources

1. <https://www.congress.gov/bill/115th-congress/senate-bill/2179/text>
2. <https://www.congress.gov/bill/115th-congress/senate-bill/2seventy-two8/text>