R Street

Free markets. Real solutions.

R SHEET ON

NATIONAL DATA BREACH NOTIFICATION

April 2021

BACKGROUND

Today we live in an era in which companies and other organizations hold significant amounts of sensitive personal and business data—much of which constitutes a treasure trove for cyber criminals and other malicious actors.

Data breach notification laws require businesses and other covered entities to notify customers in the event of a data breach. Individual laws governing breach notification practices exist in all 50 states, but there is currently no national standard.

There have been efforts to create federal legislation on this issue before. While there is federal regulation on data security in the healthcare and banking industries, other sectors, such as retail—one of the industries most targeted by malicious cyber actors—are not federally regulated in the same way. Maneuvering the existing legislative patchwork is onerous for companies that do business in more than one state, and confusing for customers who may not easily understand how their data is being protected and when they should be informed in light of a breach.

CURRENT DEBATE

Defining Data Breaches

The confusion becomes immediately evident when considering that state laws often differ on key matters, including the timelines for reporting, or even the definition of what counts as "personal data;" what security controls need to be put in place to protect said data; what constitutes a "breach;" what the deadlines are for reporting breaches; what carve outs exist; and what recourse impacted customers have. A federal data breach law would clarify the process for disclosing breaches.

Pre-emption

Some state officials, including state attorneys general, have raised concerns about federal legislation and whether it would preempt state law. Many state officials are concerned that such a national standard would prevent them from passing higher standards and developing new legislation as technology changes. However, given the costliness of complying with different state laws for companies and the lack of transparency for customers, we believe reducing regulatory burden through creating cohesive legislation is arguably more important than protecting states' abilities to incubate and innovate new laws.

SUMMARY

- Currently, each state is in charge of legislating its own data breach notification laws.
- Adopting a standardized federal data breach notification law would reduce regulatory burden.
- A federal data breach notification law could also provide valuable insight into improving our cybersecurity.

Data Sharing

Tied up in the issue of data breach notification legislation is the question of what data the government should be allowed to access for the sake of improving our nation's response to cyber threats. In 2015, lawmakers passed the Cybersecurity Information Sharing Act (CISA). The law was aimed at enhancing America's cyber posture by facilitating private companies sharing internet traffic regulation data with U.S. government agencies, particularly when the data in question is relevant to cybersecurity.

While the 2015 CISA legislation created legal cover for sharing information, many groups considered the legislation problematic. Civil liberties and privacy advocates, including the R Street Institute, were concerned about granting broad, undefined data-collection capabilities to the government and were skeptical of the law's effectiveness in fighting cyber threats.

However, there are legitimate concerns regarding the lack of data on breaches. Without a better understanding of the extent and frequencies of breaches companies experience, we leave ourselves vulnerable to future cyber attacks. A good federal data breach notification law would help improve America's cyber posture without allowing for overly broad sharing of data.

ACTION ITEMS

We agree with the recommendations of the Cyberspace Solarium Report regarding the need for a national data breach law. In order to be effective, this law will need to:

- Preempt current state data breach laws;
- Determine what level and type of intrusion counts as a "breach" and determine how and when to notify victims; and
- Establish what data should be sent to law enforcement and/or other relevant authorities and provide a method and timeline for appropriate notification.

We also believe it is important to improve our nation's knowledge regarding data breaches. In order to improve America's cyber posture, we need to know how extensive breaches are, as well as the data maturity of the organizations in question. Data regarding breaches should be aggregated and studied by a Bureau of Cyber Statistics.

CONTACT US

For more information on this subject, contact the R Street Institute, 1212 New York Ave. NW, Washington, D.C. 20005, 202-525-5717.

Tatyana Bolton
Policy Director, Cybersecurity and Emerging Threats
R Street Institute
tbolton@rstreet.org

Kathryn Waldron
Fellow, Cybersecurity and Emerging Threats
R Street Institute
kwaldron@rstreet.org