POLSINELLI

in the news

Privacy and Data Security

May 2015

Patriot Act Reauthorization Debate Delays Cybersecurity Legislation

In this Issue:

With the House of Representatives' recent action on two cybersecurity bills, focus turns to the Senate and the Cybersecurity Information Sharing Act of 2015 (CISA). Cyber attacks and data breaches are targeting some of the world's largest corporations and businesses and exposing them and their customers' data to criminal enterprises or even foreign governments. For example, two weeks ago cyber criminals stole about $5 million from Ryanair, indicating that false electronic bank transfers may be a new cyber weapon. The bills pending in Congress offer companies varying levels of liability protection for sharing information with each other and the government on cyber threats and attacks. Security experts consider such information sharing to be a vital aspect of an effective cybersecurity system. Civil liberties groups, however, are concerned that neither bill adequately protects consumer information as well as they protect businesses from liability from improperly shared (or criminally disclosed) data. As Congress continues its work on cybersecurity, businesses should be aware of the protections that may be put into place as the legislation nears final passage when considering how to best implement cybersecurity policies and procedures.

The House last week passed the Protecting Cyber Networks Act (H.R.1560) (PCNA) and the National Cybersecurity Protection Advancement Act (H.R. 1731) (NCPAA). These bills, along with CISA in the Senate, are efforts to remove the barriers to sharing information on threats, attacks and vulnerabilities to information systems, as private industry has been reluctant to share information due to concerns on legal liability, antitrust concerns, and the need to protect intellectual property and other proprietary information.

Each bill includes a provision providing a "safe harbor" from liability for companies that share cyber threat data with the Federal government. The PCNA, a product of the House Intelligence Committee, directs the Director of National Intelligence to develop procedures to promote the sharing of cyber threat data and allow businesses to develop and execute their own cybersecurity response plans. The bill allows non-federal entities to share and

receive cyber threat indicators or responses (known as "defensive measures") with other non-federal entities or specifically designated federal entities; but, the bill does not authorize non-federal entities to share information with the Department of Defense, including the National Security Agency.

The NCPAA was crafted by the House Homeland Security Committee and grants companies protection against liability for sharing data with the Department of Homeland Security (DHS) by amending the Homeland Security Act of 2002 to encourage voluntary information sharing about cyber threats, with liability protections, between and among the private sector and federal government. Specifically, the NCPAA allows the DHS' cybersecurity and communications center to include tribal governments, information sharing and analysis centers, and private entities among its non-federal representatives. NCPAA also expands the center's functions to include global cybersecurity with international partners and further requires that prior to sharing data federal and non-federal entities "take reasonable efforts to remove information that can be used to identify specific persons" and is unrelated to cybersecurity risks or incidents. During a hearing before a Senate subcommittee, DHS Secretary Jeh Johnson said that the DHS center is intended to be the primary interface of the federal government with the private sector and that he is looking to hire an "all-star" to run the center, which has not had a permanent director since last August.

In the Senate, CISA largely mirrors PCNA and is designed to encourage private companies and the government to share data to prevent and respond to cybersecurity threats. Civil liberties groups have criticized the bill and maintain that it allows companies to more closely monitor internet users and share that data with government agencies.

Industry Liability Protections and Standards

Both NCPAA and the PCNA contain liability protection for non-federal entities that share information. NCPAA's language is stronger than PCNA. The NCPAA includes language that protects non-federal entities from liability in any civil or criminal action for sharing cyber threat indicators or defensive measures, unless the entity engaged in willful misconduct. Civil liberty groups contend the bills' definition of a defensive measure is vague and does not clearly indicate what type of action a private company may take against the source of a cyber attack.

PCNA includes similar language on willful misconduct, but it also states that non-federal entities will not be held liable for the sharing or receipt of a cyber threat indicator or defensive measure *or for a good faith failure* to act based on such information that it either shared or received. This is an important distinction, as it may offer less protection than the competing "willful misconduct" standard. For instance, a consumer may be able to argue that ANY breach should be disclosed to authorities and the consumer, and that no "good faith" reason exists not to disclose a compromise. On the other hand, the willful misconduct standard poses a much higher hurdle for the consumer to clear. Some analysts are concerned that the "good faith" standard potentially exposes companies to litigation as it is more easily challenged than the willful misconduct standard. In the Senate, the CISA liability protection language is comparable to the NCPAA—both employ the higher "willful misconduct" standard, which businesses should advocate.

Legislative Timeframe

The Senate had planned to vote on CISA by the end of April, but those plans have been put on hold. Sen. Richard Burr (R-NC), chair of the Senate Intelligence Committee, has indicated there is no timetable for a floor vote on the bill. Instead, the Senate will first address the Patriot Act, which has several provisions that expire on June 1. Sen. Mitch McConnell (R-KY), the Senate Majority Leader, introduced legislation that would "fast track" reauthorization so it could be placed directly on the Senate calendar without going through the committee process. McConnell's bill would reauthorize the expiring provisions of the Patriot Act through 2020, including a provision that allows the National Security Agency (NSA) to collect bulk records of U.S. citizens' phone calls. Other senators, however, would like to amend the NSA's authorization, particularly as it relates to the agency's collection of the phone call data.

Efforts to reform the NSA have been tied to cybersecurity issues in the past and have complicated efforts to move legislation for either issue. For example, Sen. Ron Wyden (D-OR) and Sen. Patrick Leahy (D-VT), who oppose the CISA legislation, also have been critical of the NSA. The American Civil Liberties Union has criticized CISA, likening it to a surveillance bill that could expand the data used by government agencies such as the NSA.

The House voted 338 to 88 to pass the USA Freedom Act that eliminates some of the NSA's surveillance authority. The bill effectively would end the NSA's bulk collection of Americans' phone records and reauthorize the expiring provisions of the Patriot Act until December 2019. The action in the House may prompt the Senate to act on its Patriot Act bill, clearing the way for the Senate to act before June 1 on cybersecurity legislation. However, Sen. Rand Paul (R-KY) has threatened to filibuster the NSA bill.

Additional Notification Bill Expected

Outside of the three main cybersecurity measures described above, Congress is considering creating a federal standard for how and when companies must notify customers if their data has been breached. Sen. Mark Warner (D-VA) is expected to introduce legislation that would create minimum data security standards that would supersede the often conflicting state notification laws. In addition, Sen. Leahy will introduce similar legislation to require consumer notification following a breach, but unlike Warner's proposal, it would not supersede stronger state requirements.

Conclusion

After two years of debate and revision, consensus is building around the main provisions of the pending pieces of legislation. Despite the delay, the most likely outcome is that the Senate will pass cybersecurity legislation and go to conference with the House to resolve the differences. While the time frame is uncertain and can change quickly, it is expected that the Senate will pass cybersecurity legislation before the end of May.

Your business should be taking the necessary steps now to capitalize on the safe harbor provisions that appear likely to become law.

For More Information

If you or your company have questions, contact Polsinelli's Privacy and Data Security team or your Polsinelli attorney.

- George E. Kostel | *Author* | 202.626.8316| gkostel@polsinelli.com
- Darryl Drevna | *Author* | 202.626.8303 | ddrevna@polsinelli.com
- Daniel L. Farris | Co-Chair, Privacy and Data Security | 312.463.6323 | dfarris@polsinelli.com
- Gregory M. Kratofil, Jr. | Co-Chair, Privacy and Data Security | 816.360.4363 | gkratofil@polsinelli.com

To contact another member of our Privacy and Data Security law team, click here or visit our website at www.polsinelli.com > Services > Privacy and Data Security > Related Professionals.

To learn more about our Privacy and Data Security practice, click here or visit our website at www.polsinelli.com > Services > Privacy and Data Security.

POLSINELLI

real challenges. real answers. SM

About Polsinelli's Privacy and Data Security Practice

As the information economy becomes the data economy, and networks and software become more sophisticated, companies need experienced counsel to protect key data, ensure multi-jurisdictional regulatory compliance, and safeguard employee and customer privacy. Whether drafting enterprise-wide privacy policies, participating in privacy and security audits, advising on regulatory compliance, responding to a data breach, or defending against class action or other breach-related litigation, Polsinelli attorneys have the legal breach experience combined with the technical know-how to meet and exceed clients' needs.

About Polsinelli

real challenges. real answers.[SM]

Polsinelli is a first generation Am Law 100 firm serving corporations, institutions, entrepreneurs and individuals nationally. Our attorneys successfully build enduring client relationships by providing practical legal counsel infused with business insight, and with a passion for assisting General Counsel and CEOs in achieving their objectives. Polsinelli is ranked 18th in number of U.S. partners* and has more than 740 attorneys in 21 offices. Profiled by *The American Lawyer* and ranked as the fastest growing U.S. law firm over a six-year period**, the firm focuses on health care, financial services, real estate, life sciences and technology, energy and business litigation, and has depth of experience in 100 service areas and 70 industries. The firm can be found online at www.polsinelli.com. Polsinelli PC. In California, Polsinelli LLP.

* Law360, March 2014
** *The American Lawyer* 2013 and 2014 reports

About this Publication

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

POLSINELLI

real challenges. real answers. SM