THE
NATIONAL LAW REVIEW

Cyber Bulletin: Cyber-Related Legislation and Litigation

DrinkerBiddle
Article By
Steven H. Brogan
Christopher F. Petillo
Stephen A. Serfass
Nolan B. Tully
Drinker Biddle & Reath LLP
Publications

- Communications, Media & Internet
- Election Law / Legislative News
- Global

- All Federal
- United Kingdom

Monday, September 21, 2015

Federal Legislative Update

Senate Introduces Legislation on July 22 Providing Additional Authority for DHS to Supervise Federal Agencies Such as OPM

Two data breaches at the ***Office of Personnel Management (OPM)*** affecting over 20 million Americans led to a bipartisan effort to push for legislation that would provide the Department of Homeland Security (DHS) with new authority to mitigate potential threats to the computer networks of federal agencies. The legislation, titled the Federal Information Security Management Reform Act of 2015 ("FISMA"), would, among other things:

- Allow DHS to operate intrusion detection and prevention capabilities on federal agencies using the .gov domain;
- Permit DHS to conduct risk assessments of any network on the .gov domain;
- Allow DHS to enact countermeasures if and when a cyber-attack is detected;
- Bolster the authority and streamline the process for DHS to issue directives to

federal agencies, which will aid in emergency circumstances; and

- Require the Office of Management and Budget to provide an annual update to Congress on the instances in which DHS has exercised its authority to enforce government-wide cyber security standards.

FISMA would update the Federal Information Security Management Act, which was passed in 2002, and the 2014 update, titled the Federal Information Security Modernization Act of 2014.

In the wake of the significant breaches at OPM, Congress is hopeful that FISMA will help DHS mitigate the ever-changing risks and effects of continued cyber warfare. If FISMA is passed, DHS will have newly conferred authority to inspect the federal computer networks of any federal agency without needing permission from the agency or Congress. Despite the momentum that seemed to be gathering following the OPM breaches, the Senate failed to hold a vote on FISMA before the August recess and it is unclear whether a vote will be held in the coming weeks.

Federal Cyber Legislation Stagnates in Senate

As reported in the June bulletin, the House passed H.R. 1560, the Protecting Cyber Networks Act ("PCNA"), and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015 ("NCPA") in April. After the House passed those bills, the PCNA and the NCPA—both aimed at increasing the sharing of cyber threat information between the public and private entities—were packaged together and sent to the Senate. Both bills are currently stalled, as is the Senate's cyber legislation, the Cybersecurity Information Sharing Act of 2015. Despite strong bipartisan support for a federal solution to the increasingly difficult task of tracking and learning about advanced cyber threats, there has been no progress on either the House or the Senate bills. It is unclear if the Senate will address these bills in the coming months. We will report any progress in the days ahead.

Cyber Legislation Across the Pond

Proposed EU Data Protection Regulation Presents Stark Contrast to U.S. Attempts at Federal Legislation

For several years, the European Union ("EU") has been negotiating the much-anticipated General Data Protection Regulation (the "Regulation"), which will provide strict standards for data breach notification and will introduce fines for companies that suffer breaches resulting from corporate negligence. Unlike its U.S. counterpart (i.e., the 47 state Security Breach Notification Acts), the new Regulation will apply to all EU members (though member states will have some ability to add additional protections concerning certain aspects of the law). Moreover, as currently proposed, the Regulation will also give the EU jurisdiction over companies acting outside the EU that conduct business in the EU or collect data from EU citizens. One of the most notable proposed provisions is the requirement for companies suffering data breaches to notify affected persons within 72 hours if the unauthorized access to information presents a significant risk of harm. (By way of comparison, one of the shortest notice requirements among SBNAs that contain a specific time threshold is 30 days. See Fl. Stat. Ann. § 501.171(3)). Violators of the

Regulation will face a proposed fine ranging from 2% to 5% of annual global revenue if the breach results from a company's negligence.

The final version of the Regulation is expected at the end of 2015, but companies will likely have two to three years to bring their business practices into compliance before the Regulation becomes effective. At a minimum, affected entities will need to make sure their security protocols are up to date and strong. They will also need to have thorough breach response plans that anticipate the range of potential breach scenarios. Given the proposed fines for companies that negligently fail to protect individual information, companies will be well served to comprehensively test any security protocols and breach response plans, in order to identify and mitigate any potential weaknesses. US-based entities that do business in the EU should continue to monitor how the EU ultimately crafts the legislation so as to be prepared to comply with the Regulation.

Comparatively, the proposed Regulation's requirements are much stricter than current U.S. law. For example, the 72-hour breach notification standard is significantly shorter than the median 30-45 day notification standard under most U.S. state security breach notification acts. Further, even though U.S. state attorneys general can impose fines for companies that fail to enact and/or adhere to data security protocols (under HIPAA, for example), the proposed EU standard for imposing fines (negligence) and the amount of the fine (2%-5% of annual global revenue) generally exceed U.S. analogs, which require higher proof thresholds and impose lesser fines. Nevertheless, the Regulation may portend the future of U.S. data breach laws, particularly if the Regulation results in companies better adapting to evolving cyber threats and protecting personal data collected.

State Legislative Update

States Continue to Expand and Extend Security Breach Notification Acts, for Example by Requiring Risk Management Programs, and Imposing Security Requirements

On June 26, 2015, Rhode Island joined a host of other states to amend its data breach notification statute this year (which will become effective on June 26, 2016). Senate Bill S0134 amends the Rhode Island Identity Theft Protection Act of 2015 by imposing HIPAA-like risk mitigation standards and business associate agreement requirements, as well as enhanced standards governing breach notification. The new statute requires covered persons (which includes individuals and business entities) doing business in Rhode Island to implement "a risk-based information security program" that "contains reasonable security procedures and practices ... to protect the personal information from unauthorized access, use, modification, destruction or disclosure...." Covered persons must implement a document retention policy, which must demonstrate the company is only retaining PII for the minimum amount of time necessary for its business functions. Similar to the business associate agreement requirement under HIPAA, the new law requires covered persons to enter into agreements with third-party providers before sharing PII. The agreements should, at a minimum, ensure any third-party vendor implements and maintains reasonable security practices.

With respect to breach notification, Rhode Island will require notice to an affected

individual within 45 days of discovery of a breach. Rhode Island's new law also joins the growing number of states that require notification to the state attorney general if the breach affects more than 500 individuals. The new statute also expands the definition of PII to include medical or health insurance and certain email address information. Finally, the statute allows the attorney general to impose a fine of $100-$200 per record if the covered person violates the act, but only if the violation is the result of reckless conduct or willful neglect.

On June 30, 2015, Connecticut Governor Dan Malloy signed SB 949 into law, which will become effective on October 1, 2015. SB 949 was codified as Public Act 15-142, amending the state's breach notification and data security regime to include a broader definition of confidential information and strict security standards for contractors that work with state agencies. Under the new law, confidential information will include, inter alia a person's name, social security number, driver's license number; health insurance identification numbers; taxpayer identification numbers; alien registration numbers; government passport numbers; demand deposit account numbers; savings account numbers; credit card numbers; debit card numbers; and unique biometric data, "such as a fingerprint, a voice print, a retina or an iris image." Unlike other states that recently amended their breach notification standards, however, Connecticut's new law requires covered entities to report a breach to an affected individual "no later than ninety days after the discovery of the breach, unless a shorter time is required under federal law." (emphasis added). Connecticut also joins California as the only states that require companies suffering a breach to provide free credit monitoring and identity protection to affected individuals, which must be provided for at least one year. The Connecticut Attorney General has stressed, however, that his office considers this a "floor" and the office will require companies to offer credit monitoring for up to two years if the circumstances of the breach warrant the additional time.

Contractors that do business with state agencies are perhaps most affected by the Connecticut law. The act imposes strict data security requirements for such contractors, including securing servers and drives and implementing firewalls and other safeguards. Any contractor subject to the law that knows or has reason to believe confidential information has been unlawfully breached must notify the state agency with which it works and the state attorney general. Perhaps recognizing the vulnerabilities of BYO devices, the act also prohibits the storage of "confidential information" on portable devices such as a laptop, tablet, phone or other portable media without authorization from the state. If the contractor fails to comply with the new law, it can be subject to a fine.

Since the New Year, Rhode Island and Connecticut join Montana, Nevada, North Dakota, Oregon, Washington and Wyoming as states that have amended their breach notification acts. And California (SB570) and Illinois (SB 1833) are two states to watch, given the status of bills seeking to amend their respective breach notification acts. SB570 passed the California Senate on September 4, 2015, and, if adopted, would require any breach notification correspondence to specifically include the following headings and provide supporting information for each heading: (1) What Happened? (2) What Information Was Involved? (3) What We Are Doing? (4) What You Can Do. and (5) For More Information. SB 1833 has passed both houses of the Illinois Legislature and is awaiting the governor's signature. If enacted without

veto, Illinois SB 1833 would, inter alia, include geolocation data and third-party consumer marketing information in the definition of personal information; impose security requirements on entities that collect (but don't own) consumer PII; and require notification to the attorney general in 30 days after learning of a breach affecting more than 250 individuals. Simply put, there does not appear to be any slow down on the trend of states issuing new laws and/or updating older laws governing breach notification and data security.

Cyber Litigation Update

Eleventh Circuit Breathes Life into Debate Over Coverage for Data Breach Under a CGL Policy in Carolina Cas. Ins. Co. v. Red Coats Inc., No. 14-12002 (11th Cir. 2015)

The 11th Circuit's recent decision concerns coverage sought under a CGL policy for damages resulting from a data breach. The relevant facts about the underlying data breach are as follows: AvMed Inc., a Florida-based health maintenance organization and health insurance administrator, contracted with Admiral/Red Coats ("Red Coats") to provide security services for its regional offices. In December 2009, a security guard employed by Red Coats stole several of AvMed's laptop computers, one or more of which contained protected health information ("PHI") of thousands of AvMed's customers. See Carolina Cas. Ins. v. Red Coats, Inc. d/b/a Admiral Security Srvcs., Inc., 1:12-cv-00232-MP-GRJ, *2 (N.D. Fla. April 22, 2014). This incident triggered data breach notification obligations under HIPAA and state security breach notification acts. AvMed sued Red Coats for damages related to the theft, including the cost of data breach notification letters and related mitigation (i.e., two years of free credit monitoring for each affected individual), as well as damages related to defending the class action lawsuit filed shortly after breach notification letters were sent to its customers. In October 2012, AvMed and Red Coats entered into a confidential settlement agreement.

Red Coats sought coverage for the amount of that settlement from its CGL insurers, Continental Casualty Company and National Union Fire Insurance Company of Pittsburgh. In the coverage suit, Red Coats alleged it paid more than the coverage limits of the CGL policies at issue (i.e., more than $20 million) under the settlement agreement with AvMed. Both insurers denied coverage because the loss did not fall within the definition of property damage, and an electronic data exclusion barred coverage for the claims related to "data loss." Red Coats then filed suit to challenge the coverage determination.

The Federal District Court for the Northern District of Florida agreed with the insurers' coverage determination (based on the definition of property damage and the application of the electronic data exclusion) and granted summary judgment in favor of the insurers. In doing so, the court rejected Red Coats' argument that the loss of the laptops was sufficient property damage from which the data breach losses flowed. The court reasoned that the PHI was not lost or rendered unusable as required by the policy language; rather, "the problem was that it was usable and exploitable by third parties," which "is not a property damage claim." The court also noted that "there would be no coverage for the HIPAA information and any other data or programs on them, since they would represent electronic data, which is expressly excluded from coverage."

On August 17, 2015, the Eleventh Circuit vacated the lower court's judgment on the issue of whether Red Coat's settlement payment to AvMed is covered by its CGL policies, holding that the lower court failed to consider choice of law implications, specifically whether differing rules of contract interpretation between Maryland and Florida law could affect the outcome of the coverage determination. Carolina Cas. Ins. Co. v. Red Coats Inc., No. 14-12002, 2015 WL 4880523 (11th Cir. Aug. 17, 2015). In Florida, and in most states, courts construe ambiguous contract language against the insurer. In Maryland, however, courts construe ambiguous language in insurance contracts in the same manner as other contracts. The Eleventh Circuit held that whether the damages caused by the data breach were "damages because of . . . 'property damage'" could be ambiguous. Further, the court held that the electronic data exclusion contained in the policy, which excluded damages "arising out of the loss of [or] loss of use of . . . electronic data," could also be ambiguous. The lower court's failure to consider whether Maryland or Florida law applies could impact the outcome of the case, as Florida's rules of construction for ambiguous contract language benefit insureds. The Eleventh Circuit remanded the case with instructions to consider choice of law issues; whether the insurers are ultimately able to preserve their victory remains to be seen.

Red Coats is worthy of consideration because it breathes new life into the debate of whether CGL policies provide coverage for data loss and cyber events. Even as data loss and cyber exclusions continue to be integrated into CGL policy forms following the revision of ISO forms in 2014, the high stakes losses associated with cyber events (e.g., the $20+ million loss faced by Red Coats) will likely push insureds to seek coverage under CGL policies and challenge unfavorable coverage determinations—especially if they have not purchased stand-alone cyber coverage. Of course, the increased adoption of encryption technologies will continue to reduce incidences of data breaches emanating from a stolen laptop, likely limiting the usefulness of Red Coats to the plaintiffs' bar. Nonetheless, Red Coats breathes some life back into the CGL coverage debate, at least with respect to breaches related to the loss of physical media containing sensitive information.

Seventh Circuit Holds That Costs Incurred to Prevent Future Identity Theft are Sufficient to Confer Article III Standing in Remijas v. Neiman Marcus Grp., LLC, No. 14-3122 (7th Cir. 2015)

A decision issued by the Eleventh Circuit on July 20, 2015, overturning the dismissal of a data breach class action, departed from the recent trend of dismissing complaints alleging damages based on the risk of future harm such as potential identity theft. Such damages theories go directly to whether or not a plaintiff has standing to maintain suit. In order to have standing, a litigant must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." Hollingsworth v. Perry, 186 L.Ed.2d 768 (U.S. 2013). In Clapper v. Amnesty International USA, 133 S.Ct. 1138, 1146 (2013), (not a breach-related case, but one that has received significant attention from courts considering breach-related cases) the Supreme Court held that plaintiffs lacked standing because they relied on a speculative chain of possibilities, failing to show that a future injury was "certainly impending." The Court also reasoned that a plaintiff could not manufacture an injury by incurring costs implementing prophylactic measures to mitigate anticipated,

though non-imminent harm.

Post-Clapper, the plaintiffs' bar has, at times, struggled to allege injury in data breach cases sufficient to establish standing. In that way, Clapper has served as a gatekeeper against class action complaints where plaintiffs often allege speculative damages. For example, courts have rejected assertions of standing based on: (1) increased risk of identity theft; (2) costs associated with credit monitoring; (3) theft of data without allegations of misuse; and (4) reimbursed losses. See, e.g., In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., No. 12-347, 2014 WL 1858458, at *5-9, *14 (D.D.C. May 9, 2014) ("Since Clapper..., courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases ... After all, an increased risk or credible threat of impending harm is plainly different from certainly impending harm, and certainly impending harm is what the Constitution and Clapper require.").

The recent Remijas decision arguably departs from that trend. In December 2013, Neiman Marcus learned of fraudulent charges on some of its customers' credit card accounts. After conducting an investigation, Neiman Marcus discovered malware on its systems that had caused a data breach that exposed the information for up to 350,000 credit card accounts—9,200 of which were used fraudulently. Neiman Marcus sent breach notices to affected customers. Quickly on the heels of the notice being provided, several class actions were filed. In an attempt to establish standing, the class action complaints alleged an increased risk of future fraudulent charges and greater susceptibility to identity theft, as well as the costs incurred to prevent such future harm. In September 2014, the U.S. District Court for the Northern District of Illinois dismissed the case for lack of standing. Plaintiffs appealed.

A three-judge Seventh Circuit panel reversed, reasoning there is an "'objectively reasonable likelihood' that . . . injury will occur" and that "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing." The Seventh Circuit also held that mitigation costs can support injury-in-fact, where the harm is imminent, and suggested that Neiman Marcus' offer of one year of credit monitoring and identity-theft protection to all customers was "telling."

The significance of the Remijas decision is that it represents the first federal-appellate decision post-Clapper to find standing on the part of plaintiffs in a data breach class action whose damages theory rested, at least in part, on the possibility of future harm. Whether Remijas will serve as a blip on the radar or a boon to the plaintiffs' bar is still uncertain. Defense lawyers will likely highlight that some of the plaintiffs in Remijas actually experienced fraudulent charges – i.e., actual injury – and use that fact to distinguish it from cases where damages are more attenuated. Plaintiffs' lawyers will likely argue that Remijas demonstrates that the standing analysis is "fact specific," which may introduce more divergences at the district court level regarding whether prophylactic measures (e.g., credit monitoring) and increased risk of injury meet the standing requirement. There is little doubt, however, that Remijas will be influential in the data breach sphere going forward. Of course, there is a motion for rehearing before the entire Seventh Circuit currently pending (such requests are rarely granted)—and some believe the issue is headed

(again) to the Supreme Court.

Source URL: https://www.natlawreview.com/article/cyber-bulletin-cyber-related-legislation-and-litigation