Attorney Advertising

Robinson+Cole

April 23, 2015

Data Privacy and Security Insider

CYBERSECURITY

House Passes Bipartisan Bill with Liability Protections for Sharing Cyber Threat Data

In the wake of huge data breaches in the last year, multiple pieces of legislation have been introduced in the past few months relating to cybersecurity and the sharing of information between public and private entities in order to combat increasingly sophisticated cyberattacks.

Yesterday, the U.S. House of Representatives passed bipartisan legislation (the Protecting Cyber Networks Act), which is the first of several bills recently introduced to pass a vote, which provides liability protections to companies for sharing cyber threat information with each other and the government. The bill allows companies to receive protection from private and governmental regulatory enforcement actions if the company shares information about cyber threats in good faith. The purpose is to urge companies to share cyber threat information and security vulnerabilities freely so the private sector and the government can learn of new threats and combat them in a timely manner. Companies have been reticent to share details about security incidents for fear of reprisal, including lawsuits and enforcement actions based on the theory that their security is lacking or deficient. However, it is difficult to combat cyber threats uniformly and precisely if each company is experiencing the same threat, and trying to respond to it individually. If companies share their information freely without reprisal, then private industry and the government will be able to investigate the cyber threat and provide best practices to avoid and/or respond to it.

The bill gives the national Cyber Threat Intelligence Integration Center the authority to take the lead in collecting, maintaining, and sharing cyber threat information. Although the concept is logical, there continues to be criticism of the bill, particularly around providing appropriate protections for the sharing of identifiable personal information of consumers. On Tuesday, more than 50 civil liberties organizations and security experts urged legislators to reject the legislation arguing that the sharing of information threatens the privacy of U.S. citizens. They note also that due process rights will be violated by allowing multiple law enforcement agencies to use information gathered from private industry for investigations that are not related to cybersecurity efforts.

We will continue to watch pending cybersecurity legislation and update you on developments in this area.

– Linn Foster Freedman

Virginia First State to Create Cyber Sharing Organization

While the federal government grapples with multiple pieces of legislation aimed at sharing information on cyber threats, it is not surprising that states will now get into the fray.

Governor Terry McAuliffe of Virginia announced this week the creation of Virginia's Information Sharing

and Analysis Organization (ISAO), touted as a collaborative effort of the Virginia Cyber Security Commission, the Virginia Cyber Security Partnership, and the Virginia Information Technologies Agency and the private sector to collect and analyze critical infrastructure information for stakeholders to understand and combat cybersecurity risks. The effort will "help develop standards and best practices for information-sharing with the private sector."

– Linn Foster Freedman

Regulators Examining Cybersecurity Policies and Practices for the Insurance Industry

Shortly after the discovery of a cybersecurity breach at the health insurance company Anthem, Inc., the National Association of Insurance Commissioners (NAIC) called for a multi-state examination of Anthem's cybersecurity practices to determine what protections were in place and what actions could have been taken to minimize data losses. The examination is currently underway and led by insurance regulators from California, Indiana, Maine, Missouri, New Hampshire, North Dakota, and South Carolina. It should be noted that while this appears to be the first large scale multi-state examination of an insurer's cybersecurity practices, some insurance departments, such as Connecticut, have already been conducting review of an insurer's cybersecurity policies and procedures as part of its regular examinations.

Subsequently, NAIC released for comment two draft documents on cybersecurity. The first draft document, developed by NAIC's recently created Cybersecurity Task Force, is entitled "Principles for Effective Cybersecurity Insurance Regulatory Guidance" (the Principles). The Principles were designed to help state insurance departments identify cybersecurity risk and establish uniform standards to protect against it. The Principles also identify ways in which state regulators and NAIC can work with the insurance industry to flag these risks and work together on meaningful solutions.

The second draft document, developed by NAIC's Property and Casualty Insurance Committee, is NAIC's "Annual Statement Supplement for Cybersecurity Policies" (the Supplement). The Supplement reviews recent cybersecurity exposures.

In addition to NAIC's multi-state examination of Anthem, and its release of the draft Principles and Supplement, the New York State Department of Financial Services (NYDFS) is also looking into insurers' cybersecurity practices. NYDFS recently released the results of its cybersecurity survey of insurance companies. The survey inquired about insurers' current and future cybersecurity programs, including their use of third-party vendors. Forty-three insurance companies responded to the survey and provided insight into existing and planned cybersecurity programs, as well as the nature of measures taken by them to safeguard sensitive data and/or to protect against loss due to security incidents.

Links:

- NAIC's draft Principles and Supplement
- "Report on Cyber Security in the Insurance Sector," summarizing NYDFS' survey results from the insurance industry

NYDFS is the principal regulator for insurance companies operating in the State of New York, as well as certain financial entities and other financial institutions. NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories.

– Kathleen M. Porter

NAIC Provides Insurers and Regulators with Guidance on Data Security

Cybersecurity risks have become more significant as critical consumer financial and health information is increasingly stored in electronic form. On April 16, 2015, the National Association of Insurance Commissioners (NAIC) adopted guidance concerning the protection of sensitive consumer information held by insurers and insurance producers. The document also is intended to aid insurance regulators in the identification of uniform standards, to promote accountability across the entire insurance sector, and

to provide access to essential information.

The guidance consists of 12 principles that were derived from similar cybersecurity regulatory guidance issued by the Securities Industry and Financial Markets Association (SIFMA). Among other things, the NAIC indicates that state insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Further, the guidance states that regulators should mandate that these entities have systems in place to promptly alert consumers in the event of a breach.

The NAIC notes that regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, but with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations. The NAIC expects insurers, producers, and other regulated entities to join forces in identifying risks and adopting practical solutions to protect information entrusted to them, including planning for incident response and taking steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

In the wake of several recent large-scale data breach incidents, companies can expect to see more laws and regulation regarding data security on both the federal and state level. Although the concepts included in the NAIC guidance are not particularly new, insurers and other regulated entities will likely want to review the guidance to ensure that they are focusing on the same basic principles as the regulators. Companies outside of the insurance area may also find the guidance useful for their own cybersecurity efforts.

– Jean E. Tomasco

New York State Department of Financial Services Publishes Survey Results on Banking Industry Third-Party Service Providers and Cybersecurity

The New York State Department of Financial Services (NYDFS) recently published the results of its cybersecurity survey of more than 150 regulated small, medium, and large banking organizations. The survey asked for information the bank's use and management of third-party service vendors with access to sensitive information. In particular, the survey asked banks whether they conducted initial or periodic due diligence assessments of third-party vendors, and what measures vendors took to safeguard sensitive information and/or to protect against loss due to security incidents. Less than half of the banks surveyed required due diligence assessments of potential third-party vendors prior to a contract. About one-third conducted periodic assessments during the term of the vendor's contract. A third of the respondents did not require the vendor to notify them in the event of a security incident or breach.

NYDFS announced it will use the results to help it develop and adopt threshold cybersecurity standards for regulated banking organizations and their vendors. The anticipated standards will likely include due diligence, suggested or mandated vendor cybersecurity representations and warranties as well as a reporting mandate on security incidents.

Regulators, including NYDFS, continue to focus on requiring minimum cybersecurity standards to be in place when companies provide third-party vendors access to their IT systems and sensitive data. These minimum standards target identified areas of risk and are intended to reduce the number and severity of a cybersecurity incident. The particular focus on third party vendors reflects the recognition that a number of recent large scale breaches, such as those suffered Target and Home Depot, occurred in whole or part because credentials of a third-party vendor were apparently stolen.

NYDFS' survey results are available in the report "Update on Cyber Security in the Banking Sector: Third Party Service Providers," which updates its 2014 "Report on Cybersecurity in the Banking Sector" that emphasized bank's widespread reliance on third party vendors for important banking functions, such as trading and settlement operations, check and payment processing.

NYDFS is the principal regulator for state-licensed and state-chartered financial entities and other financial institutions operating in the State of New York, as well as insurance companies.

– Kathleen M. Porter

DATA PRIVACY

Sony Pictures' Hacked Emails Reveal Privileged Communications

The 2014 Sony hack is again in the news, this time highlighting the threat that data breaches pose to the attorney-client privilege. On April 16, 2015, WikiLeaks announced that it had posted and indexed hacked Sony emails. Sony is now urging media outlets to be careful with the hacked emails that contain Sony's attorney-client privilege and work product communications.

On April 17, 2015, the day after the WikiLeaks announcement, Sony's attorney, David Boies, wrote in a letter to media outlets that "the stolen data includes, but is not limited to, documents and information protected under U.S. and international legal doctrines protecting attorney-client privileged communications, attorney work product, and related privileges and protections . . .."

Boies attempted to prevent further dissemination of the privileged communications. Citing the federal Computer Fraud and Abuse Act, Copyright Act, and other state statutes concerning trade secrets and unfair competition, Boies asked for the recipients to "take all reasonable actions to prevent" their companies from "examining, copying, [or] disseminating" privileged material.

The Boies letter, however, did not stop some publications from reviewing and writing about Sony's communications with its lawyers.

This latest chapter in the Sony saga reminds us that data breaches threaten the privacy of not only a company's confidential financial and client information but also the company's confidential communications with its attorneys.

– Nuala E. Droney

Foursquare's New 'Pinpoint' Product Will Use Geolocational Data to Send Targeted Advertisements to Your Mobile Device

While Foursquare's new product, Pinpoint, surely isn't the only technology tracking your location these days, with the release of this new product, businesses can transmit targeted advertising depending on an individual's location (or the individual's locations in the past). Pinpoint, which was first announced on April 15, 2015, will send advertisements to individuals' mobile devices based on where the individual has been physically located lately … or previously located for that matter. You might be wondering, "But can they send those advertisements to me? I'm not a Foursquare user." The answer is: yes. Foursquare announced that this new product will use more than just its own databases to expand its geolocational marketing beyond its own troves of user data. But who will Foursquare get geolocational data on non-Foursquare users from? While the terms of any such agreements are not likely to become public, Foursquare does currently have relationships with third-party data partners like Microsoft, HTC, and Pinterest. As Pinpoint hits the streets we may begin to see consumer protests against this new kind of privacy invasion. We'll continue to track its use.

– Kathryn M. Sylvia

DRONE PRIVACY

FAA Approves Amazon's Second Request to Test its Delivery Drones in the Skies

While Amazon.com Inc. (Amazon) did receive approval to fly its test drones from the Federal Aviation Administration (FAA) back in March of this year for its July 2014 request, that approval proved to be useless after Amazon updated its drone technology before receiving its first approval. The FAA's drone approval process was conducted slower than the drone innovation process. But on April 10, 2015, Amazon received official approval from the FAA to test its updated aerial delivery drones. The FAA gave Amazon a two-year exemption from the federal ban on commercial drone use, but will require Amazon to follow its recently issued guidelines which require Amazon's test delivery drones to stay below 400 feet and travel no faster than 100 miles per hour. Amazon hopes to build a system by which it can deliver

products to your doorsteps in 30 minutes if you choose its Prime Air delivery. Amazon's Vice President of Global Public Policy, Paul Misener said, "We're pleased the FAA has granted our petition for this stage of R&D experimentation, and we look forward to working with the agency for permission to deliver Prime Air service to customers in the United States safely and soon." However, Misener did add that the FAA was the only organization that Amazon worked with that took longer than two months to approve its drone testing. Other organizations outside of the United States approved this testing with much more efficiency. Perhaps the FAA's guidelines are stricter than other countries, or perhaps we just aren't ready to see our Amazon packages flying above our heads just quite yet.

– Kathryn M. Sylvia

EPIC Files Suit Against FAA for Lackadaisical Drone Privacy Regulations

On March 31, 2015, the Electronic Privacy Information Center (EPIC) filed a petition against the Federal Aviation Administration (FAA) with the D.C. Circuit court asking that the court review the FAA's proposed rule on commercial drone use, which was released in February of this year, for its failure to include appropriate privacy safeguards. While the FAA did say in December 2014 that it would indeed take privacy concerns into account when drafting the proposed rule, when it finally released the proposed rule in February, the FAA explicitly stated that privacy issues were "beyond the scope of this rule making." EPIC's complaint: "to hold unlawful the FAA's withholding of proposed drone privacy rules, which Congress required the agency to issue under the FAA Modernization and Reform Act of 2012." We will follow this suit and keep you updated on its outcome.

– Kathryn M. Sylvia

ENFORCEMENT + LITIGATION

LabMD Litigation Updates

We have been following this case closely, and you can read other posts on this case and get up to speed here.

On April 16, the administrative law judge in the FTC v. LabMD case denied LabMD's request to exclude the FTC from introducing new evidence into the proceeding regarding how Tiversa Holding Corp. came into possession of LabMD's patient information. LabMD argued that the documents and evidence should be excluded as they had not been produced in response to a subpoena issued in September of 2013 and were withheld by Tiversa. The Judge indicated that the documents may be admissible on rebuttal following LabMD's presentation of its case.

In related LabMD news, the Eleventh Circuit Court of Appeals this week denied LabMD's request for an en banc rehearing relating to LabMD's claim that the FTC has exceeded its authority to regulate companies' data security practices.

The LabMD/FTC fight will come to the ring on May 5 before the administrative law judge. We will be watching it closely and will keep you up to date on developments.

– Linn Foster Freedman

HIPAA

HHS Releases HIPAA Guidance on Workplace Wellness Programs

The Department of Health and Human Services (HHS) recently issued guidance on "HIPAA Privacy and Security and Workplace Wellness Programs." The guidance helps employers determine whether or not the health information it may receive through its worksite wellness program is covered by HIPAA.

The guidance explains that in general, any health information that is created, collected and maintained,

accessed, used, and disclosed through a workplace wellness program that is part of a company's group health plan is covered by HIPAA. If the workplace wellness program is offered by an employer directly and not through the company's health plan, other laws may apply, but HIPAA does not apply.

The guidance further explains that the information relating to the workplace wellness program may not be shared with the employer as the plan sponsor without the employees' written consent or only if the employer as plan sponsor "amends the plan documents and certifies to the group health plan that it agrees to, among other things:

- establish adequate separation between employees who perform plan administration functions and those who do not;
- not use or disclose PHI for employment-related actions or other purposes not permitted by the Privacy Rule;
- where electronic PHI is involved, implement reasonable and appropriate administrative, technical, and physical safeguards to protect the information, including by ensuring that there are firewalls or other security measures in place to support the required separation between plan administration and employment functions; and
- report to the group health plan any unauthorized use or disclosure, or other security incident, of which it becomes aware."

Finally, the guidance reminds group health plans that if there is a breach of unsecured PHI, it is obligated under the HIPAA breach notification requirements to notify the individuals, the Office for Civil Rights, and potentially the media of the breach.

Employers may wish to review the guidance and their HIPAA compliance regarding worksite wellness programs. The short guidance can be accessed here.

– Linn Foster Freedman

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy and Security Team.
