Wednesday, January 28, 2015

Cybersecurity: the view from Washington

Jeramie D. Scott *is the national security counsel and privacy coalition coordinator for the Electronic Privacy Information Center (EPIC). His work focuses on the privacy issues implicated by domestic surveillance programs with a focus on cybersecurity, big data, drones, biometrics and license plate readers. Mr. Scott also runs the monthly Privacy Coalition meeting that brings together representatives of consumer and privacy organizations with key Washington decision makers in the privacy field.*

Following the recent Sony hack and ongoing concerns about the vulnerability of computer systems in the U.S., both President Barack Obama and Congress are moving new proposals for cybersecurity. In the State of the Union speech last week, Obama called on "Congress to finally pass the legislation we need to better meet the evolving threat of cyber attacks." The president also proposed cybersecurity legislation that promotes "better cybersecurity information sharing between the private sector and government ... and information sharing amongst the private sector." The Sony hack and other data breaches have focused attention back on cyber threat information sharing, but the real culprit - more often than not - is inadequate security measures.

The call for increased cybersecurity information sharing is not new. The House of Representatives in both the 112th and the 113th Congresses passed the Cyber Intelligence Sharing and Protection Act (CISPA), although the Senate never considered the bill. Both times CISPA was introduced, privacy and civil liberties advocates opposed the act because the vague language threatened to open up a floodgate for government access to user information without judicial oversight. Both times the House faced a veto threat from the president, based on the lack of privacy and civil liberties protections.

Despite the earlier opposition to the House measure, Obama is now actively urging Congress to pass CISPA-style legislation. The president's cyber information proposal, in large part, mirrors the CISPA legislation recently reintroduced by Rep. C.A. Dutch Ruppersberger, but there are key differences. Notably, the president's proposal requires companies to remove personally identifiable information prior to transferring it to the government. The hope is this safeguard will address the concerns of civil liberties groups and others.

The reintroduced CISPA (House Resolution 234) is identical to House Resolution 624, the bill that passed the House last Congress. Like H.R. 624, the new proposal raises several issues: (1) The broad definition of "cyber threat information;" (2) the lack of any requirement for the private sector to strip out needless personally identifiable information; (3) the leeway the private sector is granted to identify and obtain cyber threat information; and (4) the immunity the private sector receives as long as companies "act in good faith."

The definition of "cyber threat information" includes information pertaining to: a network vulnerability; a network integrity threat; efforts to deny access to a network; and efforts to gain unauthorized access. What exactly constitutes a vulnerability or a threat is not defined, but left up to the private sector to interpret. With such broad liability protection, the private sector has no incentive to interpret "cyber threat information" narrowly. Companies will have incentive to divulge unwarranted amounts of information about their networks (including user information) in the hopes to better

SPECIAL REPORT
20 Under 40

Thursday, January 29, 2015

Criminal
Brady violations gain judicial attention as well as proposed solutions
A plan to rein in prosecutors who hide favorable evidence from the defense in criminal trials could be gaining traction, lawyers and judges said.

Litigation
Prepaid mobile phone carrier to pay $40 million to resolve FTC suit
TracFone Wireless Inc. slowed down Internet speeds when users went over a certain data limit, even though they were told their plans were unlimited, the Federal Trade Commission announced Wednesday.

Law Practice
The origins of the modern law firm
Consider that in 1970, the largest law firm was Shearman & Sterling, with 164 attorneys. By 1985, Shearman & Sterling had 432 lawyers. Today, Baker & McKenzie has over 4,000. By **Edwin B. Reeser**

Bankruptcy
Bankruptcy cases decline 13 percent in 2014
The continuing drop in bankruptcy cases points to economic recovery, but attorneys with boutique firms say the trend is hurting business.

Mergers & Acquisitions
Dealmakers
A roundup of recent transactions across the state and the lawyers involved.

Corporate Counsel
John F. Schultz
Executive Vice President and General Counsel
Hewlett-Packard Co. Palo Alto

Securities
Judge tosses charges against investment bank
A LA Superior Court judge on Tuesday dropped charges against Shattuck Hammond Partners LLC in a case brought by dozens of investors duped in a Ponzi scheme masterminded by a convicted felon who illegally sold $200 million in securities.

protect business from cyber threats.

The potential for excessive disclosure is compounded by the lack of a requirement to remove personally identifiable information. In the House measures, companies are not required to strip out personal information. Again, CISPA protects companies from any liability, so the private sector will use only the minimal effort needed to disclose the information. What CISPA encourages is the aggressive pursuit of cyber threat information.

With little guidance on the limits for obtaining cyber threat information and built-in immunity, companies may enter a legal gray area as they aggressively pursue cyber threat information. Companies have the right to protect their network and computers. It is less clear whether companies may pursue threats beyond their own networks and computers. Can they follow a cybercriminals trail and hack the criminal's computer to obtain cyber threat information? Can companies purposely setup "honey pots" to entice would-be hackers to steal documents implanted with beacons indicating the documents location (i.e., IP address)? What if the hacker routed his attack through your computer? Is your information fair game for disclosure to the government? The answers are not clear and CISPA provides no guidance.

The risk with CISPA is that it will allow government surveillance of private communications outside the bounds of traditional wiretap law. Although the Department of Homeland Security and the Department of Justice are the designated agencies to receive the cyber threat information disclosed by the private sector, the act requires the information to be shared in real time with other agencies with a national security mission. This would, broadly speaking, encompass the entire Intelligence Community, including the National Security Agency.

Despite the repeated calls for CISPA, it's not clear that the legislation is necessary. First, private companies already disclose user information to each other regarding cybersecurity threats. And companies can use nondisclosure agreements to protect their commercial interests in their data. Second, the government already transfers cyber threat information to the private sector. Years ago the government set-up a voluntary sharing program with defense contractors whose work by nature includes sensitive and often classified information. Over the years, the voluntary program has steadily expanded to other companies and sectors, as documents obtained by the Electronic Privacy Information Center (EPIC) under the Freedom of Information Act reveal. Third, most importantly, more needs to be done to improve security practices. That is the glaring lesson of the recent hacks.

The hacks of Sony, Home Depot, and many others would not have been stopped with increased disclosures of user data to the government. The hacks may have been prevented with better security measures, such as data minimization, two-factor authentication, encryption, and other practical security measures. Cybersecurity policies that encourage the adoption of best practices, rather than those that rely on the bulk release of user data, may be the best policy going forward.

Jeramie D. Scott *is the national security counsel and privacy coalition coordinator for the Electronic Privacy Information Center (EPIC). His work focuses on the privacy issues implicated by domestic surveillance programs with a focus on cybersecurity, big data, drones, biometrics and license plate readers. Mr. Scott also runs the monthly Privacy Coalition meeting that brings together representatives of consumer and privacy organizations with key Washington decision makers in the privacy field.*

\\ladj008/DJICText/News/Text/1061527D01282015I7.htm
Editorial Id: 939462
Publication Date: 01/28/2015

Corporate
Chinese entertainment company taps Stroock in $1.5B deal with Lions Gate
The deal, observers said, is emblematic of the increasing attention Chinese investors are giving to U.S. movie producers and distributors amid a rapid expansion of China's film market.

California Courts of Appeal
Kickback lawsuit against Memorial Coliseum rave promoters resurrected
An appellate court will not let a suit regarding Los Angeles Memorial Coliseum rave revenues go quietly into the night.

Constitutional Law
Is there new life for Proposition 8?
The U. S. Supreme Court's grant of certiorari in *Obergefell v. Hodges* on Jan. 16 signaled the court's intention to finally decide whether states may bar same-sex marriages. By **Karl Manheim, John S. Caragozian and Donald Warner**

Technology & Science
A more draconian computer fraud act?
While President Barack Obama in his State of the Union address announced a cybersecurity legislative proposal to clarify the Computer Fraud and Abuse Act, it is unlikely that will satisfy the statute's many critics. By **Peter J. Toren**

Health Care & Hospital Law
FDA's general wellness guidance is welcome news
The FDA just issued a draft guidance which sounds like good news for manufacturers and distributors of "low risk products that promote a healthy lifestyle." What does that mean for industry? By **Michael H. Cohen**

Law Practice
Who, me? Law firm partners, profits and payroll taxes
These days, being a partner in a law firm may not mean what it used to mean. Specifically, in law firms, at least, being named "partner" may not mean ponying up capital. By **Robert W. Wood**

Communications
Transparency is critical when using native advertising
Attorneys from the FTC's advertising division said the FTC will be providing guidance on how native advertisements can comply with regulations. What does that mean for businesses? By **Ronald R. Camhi and Andrew Howard**

Judicial Profile
Brad M. Fox
Superior Court Commissioner Los Angeles County (Torrance)

Litigation
A slow start for expedited jury trials
The goal when expedited jury trials became an option in 2011 was to streamline certain civil cases by limiting trials to an 8-hour day, saving time and

money. But since then only a small number of cases have been tried this way.