Cybersecurity Policy Report - April 18, 2011

Table Of Contents

WHITE HOUSE ROLLS OUT PLAN FOR SECURE ONLINE IDENTITIES

The White House this week unveiled its long-awaited proposal for a regulatory framework to encourage the private sector to create a more secure Internet identity ecosystem for businesses and consumers. The administration hopes that improving online identity security will reduce online fraud and theft and lead to growth in online business transactions and the entire economy.

The administration's National Strategy for Trusted Identities In Cyberspace (NSTIC) aims to establish standards for online identity authentication and forms the centerpiece of its strategy to improve online security for those who want to take advantage of it. Development of the identity authentication standard was one of the steps called for in the White House's 2009 Cyberspace Policy Review. The administration issued a draft version of the NSTIC in June 2010, and it has been working its way through an interagency review process since then.

Central to the trusted identities effort is enabling consumers to create, through private sector companies, a single online identity that could be used for all online transactions and that would reveal to the consumer's online counterparty only as much information as necessary to conduct a specific transaction. A banking transaction, for example, would require a greater degree of identity information than would buying a movie ticket.

The trusted identity credential mechanism could take the form of software on a smart phone, a smart card, or a token that generates a one-time digital password, the administration said in its April 15 unveiling of the plan.

Businesses will benefit from the trusted identity system, the administration said, because it will allow them to more easily do business online and avoid the cost of building their own login systems.

"By making online transactions more trustworthy and better protecting privacy, we will prevent costly crime, we will give businesses and consumers new confidence, and we will foster growth and untold innovation," President Obama said.

Commerce Secretary Gary Locke said, "We must do more to help consumers protect themselves, and we must make it more convenient than remembering dozens of passwords." At an event to announce the NSTIC release, he said a significant share of cyber crime resulted from consumers using the same passwords to access multiple sites.

On privacy issues, the NSTIC proposal remains a work in progress. Administration officials said their strategy sought to create tougher online privacy protections, and the National Institute of Standards and Technology will hold a series of workshops later this year for stakeholders to hammer out policy suggestions on privacy, interoperability, and other issues.

"Working together, innovators, industry, consumer advocates, and the government can develop standards so that the marketplace can provide more secure online credentials, while protecting privacy, for consumers who want them," Mr. Locke said.

Mr. Locke and other officials repeatedly stressed that neither the government nor the private sector would require consumers to get a trusted identity credential in order to undertake online transactions. They were responding to the notion that has taken hold in some quarters that the NSTIC would create a national Internet identity card.

Many groups, however, praised the proposal. The U.S. Chamber of Commerce, which hosted the event at which the proposal was unveiled, praised its reliance on the private sector to create the new credentials and its prospects for reducing online fraud. "The strength of our free enterprise system is directly tied to the prosperity and security of the Internet," said Ann Beauchesne, the chamber's vice president-national security.

Sen. Barbara Mikulski (D., Md.), chairman of the Senate Appropriations subcommittee on Commerce, Justice and science and a leader on cybersecurity issues, said she would "use my expertise and clout to stand sentry over and secure the $25 million" that the Obama administration has requested for fiscal year 2012 to fund the NSTIC effort.

"This is a call by the administration to the private sector to step up, take leadership of this effort, and provide the innovation to implement a privacy-enhancing, trusted system," said Leslie Harris, president of the Center for Democracy & Technology. Added CDT's Aaron Brauer-Rieke, "We deserve better control over our identity and more confidence in our transactions online." -- John Curran, john.curran@wolterskluwer.com

WHITE HOUSE's CYBERSECURITY REQUESTS TO INCLUDE ENHANCED HACKING PENALTIES

A package of cybersecurity proposals that the White House will soon deliver to Congress will request data breach legislation and a "streamlining and strengthening" of the hacking penalties provided by the Computer Fraud and Abuse Act, lawmakers were told this week.

"This administration is committed to implementing a comprehensive framework that will allow us to bring all appropriate tools -- criminal and otherwise -- to bear against cyber criminals, terrorists, and other malicious actors," said Jason Weinstein, a deputy assistant attorney general at the Justice Department.

Testifying April 12 before the Senate Judiciary Committee's subcommittee on crime and terrorism, Mr. Weinstein assured lawmakers that the administration would soon produce a cybersecurity policy blueprint for Congress.

"There's an interagency process that's moving at a fever pitch. I wouldn't say it's been at a fever pitch throughout its life, but in the last six weeks, it has," he said. "We've got people who are literally working around the clock, judging by the time at which they're e-mailing me in the middle of the night, to try to get proposals ready to present to you, and I think that will happen very soon."

Senators had complained that their work on cybersecurity -- involving seven committees and producing a handful of competing bills -- was being hampered by the administration's lack of engagement. "We're long overdue for the president to share his proposals for cybersecurity legislation so that we can get started," said Sen. Jon Kyl (R., Ariz.), the subcommittee's ranking member.

The proposals that the White House is considering, Mr. Weinstein said, include boosting the penalties for computer crimes in the Computer Fraud and Abuse Act, a 1986 law that was most recently updated in 2008. "That proposal is still baking, and when it's fully cooked we'll be pleased to bring it to you."

Another likely proposal would address corporate data breaches that expose the personal information of customers. "Right now there are 47 individual state data breach requirements, all of which are unique and all of which have different reporting requirements," said Pablo Martinez, deputy special agent in charge of the U.S. Secret Service's cyber crime operations.

"It's important for us to create a national data breach bill so that we don't continue to have this myriad" of state laws, Mr. Martinez told the subcommittee. Companies that lose data "should not only notify consumers or the victims . . . but they also should notify the government," he said.

The proposed bill would create a "safe harbor" for companies that took adequate steps to prevent data breaches to protect them from civil lawsuits, he added.

The administration officials were also urged to consider allocating more resources to combating cyber attacks. "Even in this time of budget-cutting, given the enormous stakes, the cyber threat is simply too dangerous to under-resource," said Sen. Sheldon Whitehouse (D., R.I.), the subcommittee's chairman.

He noted that the Justice Department had nearly 90 attorneys dedicated to fighting traditional organized crime and hundreds assigned to drug enforcement but only 40 in its computer crimes unit.

"We are on the losing end of the biggest transfer of wealth in the history of humankind through [cyber] theft and piracy," he told Mr. Weinstein. "It strikes me that having fewer attorneys dedicated to computer intrusions . . . than are dedicated to old-fashioned organized crime is a sign that we here in Congress need to provide you more resources to focus on the cyber threat."

Mr. Weinstein explained that many of the attorneys in the organized crime unit pursued cyber cases because cyber criminals were part of crime syndicates. In addition, he said, attorneys in DoJ's fraud division and other units also handle cyber cases.

But he agreed with Sen. Whitehouse and noted that the president's proposed 2012 budget included funding for six additional attorneys in the cyber crime section. "It is really undeniable that the scope of the problem, which is growing every day, far outpaces the resources that are available to pursue it," he said.

Another witness, however, suggested that the addition of six attorneys at DoJ was a feeble effort to counter the cyber threat. "Six more prosecutors are not going to address this issue in any significant way," said Stewart Baker, a partner at Steptoe & Johnson LLP and a former assistant secretary in the Department of Homeland Security.

"Law enforcement, in my view, is almost entirely helpless at this point," Mr. Baker told the subcommittee. "Many things that we hope will save us will not."

He suggested, among other things, that anonymity on the Internet should be minimized to make it easier to locate attackers. "We cannot solve this problem if we cannot realistically threaten to punish the people who are carrying these attacks out," he said.

The private sector is unprepared to protect its trade secrets and is "utterly clueless" about the possibility of cyber sabotage, he added. "They don't want to think about the possibility of sabotage because they have no idea what to do about it." -- Tom Leithauser, tom.leithauser@wolterskluwer.com

UPCOMING LEGISLATION TO FOCUS ON CLOUD, GLOBAL CYBERSECURITY

Three bipartisan bills that will attempt to address various cybersecurity issues, from international cooperation to cloud computing, will be introduced soon in the Senate, lawmakers said this week.

First, Sens. Sheldon Whitehouse (D., R.I.) and Jon Kyl (R., Ariz.) announced they were working on a cybersecurity "awareness" bill. "While this bill may be considered chiefly a placeholder for things to come, it's an important step because of the multitude of topics it covers," Sen. Kyl said.

Sen. Whitehouse is chairman of the Judiciary Committee's subcommittee on crime and terrorism, and Sen. Kyl is its ranking member.

A second bill -- to address policy issues associated with cloud computing -- will be introduced by Sens. Amy Klobuchar (D., Minn.), chairman of the Commerce, Science, and Transportation Committee's subcommittee on competitiveness, innovation, and export promotion, and Orrin Hatch (R., Utah).

"Cloud computing has the potential to alleviate some of the concerns in the cybersecurity field, particularly introducing economies of scale and making sophisticated protection available," Sen. Klobuchar said. "However, it also raises unique diplomatic issues because data is being stored in several different countries."

The third bill announced this week will be a reprise of legislation introduced last year by Sen. Hatch and Sen. Kirsten Gillibrand (D., N.Y.) that would encourage other nations to crack down on cyber crime (CPR, March 29, 2010). -- Tom Leithauser, tom.leithauser@wolterskluwer.com

HOUSE PANEL TOLD TO CLARIFY LEGALITY OF DATA SHARING TO BOOST CYBERSECURITY

Clarifying the legal questions surrounding sharing of threat "signatures" among public and private entities could significantly improve efforts to secure telecom networks and other types of critical infrastructure, a senior AT&T official told lawmakers at an April 15 hearing.

In a hearing held by the House Homeland Security subcommittee on cybersecurity, infrastructure protection, and security technologies, Edward Amoroso, senior vice president and chief security officer at AT&T, Inc., said one key problem was the difficulty of information-sharing about threat "signatures" between the public and private sectors. When the prospect of sharing information with the government arises, a "team of lawyers" gets involved and complicates the process, he said.

In terms of the government providing a threat signature to a carrier, Mr. Amoroso said there was a "tremendous lack of clarity about whether that is legal or not." Some say it can be done, and others say it cannot, he said. Because of AT&T's conservative nature, it generally will not take actions that are legally murky, he said.

"Anytime sharing information is proposed, there's a big debate about each and every situation," Mr. Amoroso said. "We need a framework that gives us some more leeway."

Asked what could be done to fix the problem, Sean McGurk, director of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security, said his agency was "sharing information -- but not signatures." Mr. McGurk said signatures "may be system specific or product specific," so instead his group "routinely" publishes "indicators," which he said can be used to "generate those signatures that are specific to those pieces of equipment."

Subcommittee Chairman Daniel Lungren (R., Calif.) said a key to improving cybersecurity would be to increase market demand for secure products and services. "How do we make it bottom-line relevant for both individuals and businesses?" he asked.

One thing the government could do is "lead by example," Mr. Amoroso replied. For example, General Services Administration security policies are "applied somewhat unevenly," he said. "One of the responsibilities of government is, I think, to first look inward . . . and to show by example that not only is this important, but that it can be done."

In addition, some companies "don't see it as urgent" that they protect their networks, Mr. Amoroso said. More troublesome is that even if they saw cybersecurity as urgent, many are "not sure what to do about it," he said.

"Once we get our arms around some techniques that seem to work, the technology has already changed," Mr. Amoroso said. The pace of change "makes it extremely difficult because the challenge changes so rapidly." -- Brian Hammond, brian.hammond@wolterskluwer.com

CHINESE CYBER ATTACKS ERODE U.S. SECURITY, LAWMAKERS TOLD

Witnesses at an April 15 House subcommittee hearing offered a sobering assessment of the impacts of coordinated cyber attacks and cyber espionage allegedly undertaken by the Chinese government against the U.S., stressing that the economic and national security of the U.S. required better cyber defenses.

During a hearing on "Communist Chinese Cyber-Attacks, Cyber-Espionage, and Theft of American Technology" held by the House Foreign Affairs subcommittee on oversight and investigations, Chairman Dana Rohrabacher (R., Calif.) said China was launching thousands of cyber attacks on U.S. assets every year.

"Outsourcing of computer and consumer electronic production to China, not only by American but also by Japanese, Taiwanese, German, and South Korean firms, has helped create a Chinese cyber threat that now compromises the security of the Western world," he said.

Panelists detailed a wide range of technologies that they said China had developed as a result of stealing information from the U.S., ranging from computer and information technology systems to commercial and military aircraft.

Pat Choate, director of the Manufacturing Policy Project, said stealing technology was "far easier and cheaper than doing original research and development." A particular concern cited by Mr. Choate was attacks on the "open computers of the U.S. Patent Office -- a cyber spy can find virtually all the newest, cutting-edge U.S. technologies in virtually any field." He said the U.S. Patent Office had old computers and technology, making it a particularly easy target.

Rep. Russ Carnahan (D., Mo.) asked panelists to assess the "willingness to engage with us regarding cyber threats and technology threats." Mr. Choate replied, "We must assume as a policy that not only China but Germany and Brazil and other countries are out to steal our technology. It's our obligation to not make it easy as we do now."

Richard Fisher, senior fellow-Asian military affairs at the International Assessment and Strategy Center, said, "I don't see that the Chinese government today shares any interest in partnering with us in an effective way."

"They're not going to be interested in talking to us until they have reached a level of power with which they are comfortable," he testified. "Once they gain a position of superiority, they're going to want to start dictating the rules, changing the rules." -- Brian Hammond, brian.hammond@wolterskluwer.com

TOP TELECOM, CABLE GROUPS ISSUE CYBERSECURITY LEGISLATIVE PROPOSAL

The U.S. Telecom Association, the National Cable & Telecommunications Association, and CTIA have proposed a "legislative framework" designed to strengthen the security of the nation's broadband networks. Their recommended steps include establishing a central federal government cybersecurity organization and structure, engaging in a partnership with private network operators, improving user education, and conducting a thorough analysis of the threats and costs of action before moving forward with any major cybersecurity initiatives.

In an April 14 letter to White House Cybersecurity Coordinator Howard Schmidt, the groups said their proposal "provides for improvements in the government's own cybersecurity posture, addresses national security issues through strong partnerships between government and all of the relevant private-sector stakeholders, and calls for robust consumer and business education

to thwart online threats."

Along with the letter, the groups sent a six-page document detailing their proposed framework for cybersecurity legislation. According to that framework, Congress should focus on three key priorities: (1) improving the government's own cybersecurity posture; (2) addressing national security issues through "strong partnerships with industry"; and (3) improving consumer and business users' "capacity to thwart online threats."

To address security of government networks, the framework recommends streamlining and centralizing cybersecurity organization and structure. It also recommends the use of the government's acquisition policy as a "powerful tool for pushing vendors" to develop capabilities to ensure government networks are as secure or more secure than private networks. The government also should improve federal civilian training and certification and increase research and development efforts, the groups said.

To develop a partnership with industry, the groups recommended several steps. First, the government should seek to develop a "real partnership, not a series of unfunded mandates," they wrote. "Unfunded technical mandates, rigid response requirements, and command-and-control type governance structures in cyberspace must be avoided."

"The development of a cybersecurity policy that emphasizes best practices and flexible response mechanisms would ensure that infrastructure owners retain the ability to implement all measures available to them to secure their network and systems," they said.

In addition, government responses to national emergencies must be conducted "in close coordination with industry," the framework suggests. "Critical infrastructure owners must retain the freedom and flexibility to implement those measures that they deem appropriate to secure their networks and systems and to protect their customers," the groups wrote. "A response plan that slows industry's response time to hostile cyber activity could be disastrous."

They also recommended that the designation of "critical" information infrastructure should be the result of joint work involving the government, network operators, "major edge providers, and other key stakeholders in the Internet ecosystem." The groups said they opposed "duplicative and/or burdensome analytical and reporting requirements." They suggested offering incentives to promote "enhanced cybersecurity compliance" and recommended that the government facilitate "appropriate information sharing."

As for the third key priority, improving user education and preparedness, the groups suggested that the government fund K-12 education efforts to "prepare young Americans to engage in cyber-related best practices" and increase funding for college-level programs on "all aspects of cyberspace, not just software programming or computer science."

But before any new cybersecurity measures are developed, Congress should "ensure that a proper analysis is conducted of all relevant factors including, for example, the nature of the problem and its origins, any corresponding solutions and a measure of their effectiveness, costs associated with implementing such solutions and the rightful bearers of such costs, and the potential for counterproductive or harmful consequences that could follow implementation," the groups said.

"While that analysis is being done, the government should continue to work closely in partnership with private industry to identify critical infrastructure and to promote practices that facilitate quick and effective responses to cyber threats," they added.

"Secure networks are essential to protecting our customers, and thus no one is more committed to effective cybersecurity than our member companies," USTelecom, NCTA, and CTIA wrote in their letter to Mr. Schmidt. "We hope you will review our recommendations and incorporate them into the administration's forthcoming recommendations to Congress."

"We stand ready to work with both the administration and Congress to enact cybersecurity legislation premised on the attached framework," they said. "We believe that by doing so, you will help to create a stronger and safer broadband experience for all Internet users and for the nation's security as a whole." -- Brian Hammond, brian.hammond@wolterskluwer.com

CONGRESS URGED TO AVOID EFFORTS TO REGULATE 'CLOUD'

Capitol Hill would be wise to keep its hands off of cloud computing as that technology develops, industry officials said this week. But they admitted there were significant questions that needed to be answered as the sector continued to evolve, specifically in the areas of privacy and security.

Speaking at an April 5 forum sponsored by the Congressional Internet Caucus, industry experts acknowledged there were risks involved with cloud computing. But many of those could be overcome by educating consumers, they said, and they expressed confidence that existing rules could address any potential problems.

Allan Friedman, governance studies fellow and research director with the Brookings Institution's Center for Technology Innovations, said it would be best, for now, if government got out of the way. "We need to make sure that when a company has

data online, they have certainty," he said. "And right now, they are lacking that."

Several others agreed. Dan Burton, senior vice president-global public policy at Salesforce.com, said it was "premature for Congress to be passing legislation." David Valdez, CompTIA's senior director, said increasing public awareness about the technology would be the best way to avoid problems. "Really what we need is to educate consumers on what the implications are . . . if they put their information in a cloud environment," Mr. Valdez said.

If government decides to weigh in, it should take a wide view of cloud computing, the forum participants said. The average person might think of Facebook or Twitter when they think of cloud applications, but a host of small businesses already run their operations using the cloud, said John Calhoun, managing partner at OnPoint Consulting. "Let's have a broad perspective on this when it comes to cloud," he said.

Longer term, however, several issues will have to be addressed, including how to deal with overseas data storage, privacy, and security, officials said. -- Ted Gotsch, ted.gotsch@wolterskluwer.com

KERRY, McCAIN PRIVACY LEGISLATION DRAWS INITIAL SUPPORT FROM INDUSTRY, CONSUMERS

Sens. John Kerry (D., Mass.) and John McCain (R., Ariz.) have introduced legislation designed to provide a "bill of rights" governing the collection, use, and dissemination of consumers' personally identifiable information (PII). The legislation drew initial support from telecommunications service providers and major consumer groups.

The "Commercial Privacy Bill of Rights Act of 2011" would require collectors of information to implement security measures to protect that information. The bill would provide consumers with rights to "notice, consent, access, and correction" of their information.

Any party collecting information would be required to provide "clear notice to individuals on the collection practices and the purpose for such collection," according to a summary of the bill. It also would require the collector of information to enable an individual to opt out of any information collection and require an opt-in option for collection of "sensitive" PII.

The bill would require "robust and clear notice" to individuals of their ability to opt out of the collection of information for the purpose of transferring it to third parties for behavioral advertising. It also would mandate that consumers have the ability to access and correct information or the ability to request that it no longer be used or distributed.

Parties gathering information also would be limited to collecting "only as much information as necessary to process or enforce a transaction or deliver a service," but the bill would "allow for the collection and use of information for research and development, to improve a transaction or service, and require that the information is only retained for a reasonable period of time."

The bill would put enforcement in the hands of state attorneys general and the Federal Trade Commission, but would bar simultaneous enforcement by both the FTC and a state AG. The bill would cap the fines an AG could seek for a violation and would prevent private rights of action.

Voluntary "safe harbor" programs also would play a part in the regime outlined in the legislation. The bill would allow the FTC to approve nongovernmental organizations to oversee voluntary safe harbor programs, as long as they achieve protections "as rigorous or more so as those enumerated in the bill." The bill would direct the Department of Commerce to convene stakeholders for the development of applications for safe harbor programs to be submitted to the FTC.

Sen. Kerry, chairman of the Senate Commerce, Science, and Transportation Committee's subcommittee on communications, technology, and the Internet, said Americans had "a right to decide how their information is collected, used, and distributed and businesses deserve the certainty that comes with clear guidelines."

"Our bill makes fair information practices the rules of the road, gives Americans the assurance that their personal information is secure, and allows our information-driven economy to continue to thrive in today's global market," Sen. Kerry said. "This is a win for bipartisanship, a win for consumers, a win for the Internet, and a win for businesses online and off. Most importantly, in a Washington where partisanship and division too often triumphs, it's a victory for common sense."

Sen. McCain said the legislation would establish "a framework for companies to create such an environment and allows businesses to continue to market and advertise to all consumers, including potential customers." The bill, however, does not allow for the "collection and sharing of private data by businesses that have no relationship to the consumer for purposes other than advertising and marketing. It is this practice that American consumers reject as an unreasonable invasion of privacy."

Initial reaction to the legislation from telecommunications carriers as well as consumer groups was largely positive.

Tim McKone, executive vice president-federal relations at AT&T, Inc., congratulated Sens. Kerry and McCain for their "bipartisan

leadership in establishing a thoughtful and comprehensive legislative framework to address individual privacy in the Information Age."

Mr. McKone said that in particular, AT&T was "gratified that the Commercial Privacy Bill of Rights Act of 2011 both recognizes and specifically addresses the potential for overlapping regulation of communications providers by multiple federal agencies and establishes a solution that eliminates wasteful and inefficient regulatory duplication."

Peter Davidson, senior VP-federal government relations at Verizon Communications, Inc., said Verizon had a "long-standing commitment to privacy as a consumer-trust issue; any new privacy rules must be focused on protecting consumers' data, not the technology used to collect the data."

Mr. Davidson called the proposed framework a "great start toward modernizing privacy rules for the Internet age, and moves us closer to a one-stop shop for consumer protection. Policy-makers and all those invested in the issue should continue to develop privacy principles with the consumer in mind, while allowing continued growth and innovation across the Internet marketplace."

"As an industry that already provides its customers with the highest levels of privacy protection, we believe consumers will benefit from legislation that requires all players in the Internet economy to adhere to a common set of rules implemented by a single regulator," said Walter McCormick, president and chief executive officer at USTelecom. "While we are still reviewing the bill introduced today by Sens. Kerry and McCain, it appears they have taken a big step in that direction, and we appreciate their efforts."

James Assey, EVP at the National Cable & Telecommunications Association, said the legislation "appropriately focuses attention on the need for a level playing field with respect to privacy regulation." He added that "further review is warranted to ensure that such legislation not only addresses reasonable privacy interests but also supports a healthy marketplace for content creation and digital services."

Ioana Rusu, regulatory counsel for Consumers Union, called the bill an "important step forward in giving people more control over their personal information online. For the first time, all businesses would have to operate under consistent, mandatory standards for online privacy protection. To us, that's progress."

Susan Grant, director-consumer protection at the Consumer Federation of America, said, "We hope that this is a foundation that we can build on to give consumers the privacy protections they need."

"Sens. Kerry and McCain have shown impressive leadership in putting forward a bipartisan bill to address the privacy concerns of the 21st century," said Leslie Harris, president of the Center for Democracy and Technology. "The bill contains many strong elements, and we look forward to working with the senators and the members of the commerce committee to create an enduring, flexible privacy framework that protects consumers while encouraging companies to innovate."

Daniel Castro, senior analyst at the Information Technology and Innovation Foundation, said the bill "correctly recognizes that a balance must be struck between regulations that slow down innovation and those that protect consumers." Mr. Castro said ITIF also agreed that commerce should "take the lead on crafting data policies that can foster beneficial types of data-sharing."

"As ITIF has written previously, the goal of any privacy legislation should be to protect consumers while fostering competition, choice, and innovation," Mr. Castro said. "While the ideal privacy legislation would focus on protecting consumers from harm rather than legislating data-handling requirements, the legislation introduced today does provide a co-regulatory framework that allows industry to partner with government to potentially create more flexible rules for businesses that could help reduce the negative impact on the Internet ecosystem."

Mr. Castro, however, warned that "all of the economic evidence suggests that strict privacy regulations can have a negative impact on the Internet ecosystem." Policy-makers should "carefully consider the potential economic consequences of certain requirements, such as data minimization, that restrict current business processes, do not harm consumers, and can lead to the development of new products and services," he said.

"Congress should also take the time to assess the efficacy of current enforcement mechanisms and the progress of industry self-regulatory efforts launched late last year before enacting potentially new policies that might impair these efforts," he added. -- Brian Hammond, brian.hammond@wolterskluwer.com

STEARNS PRIVACY BILL WOULD OFFER 'OPT-OUT' FOR THIRD-PARTY DATA USES

Reps. Cliff Stearns (R., Fla.) and Jim Matheson (D., Utah) this week introduced consumer privacy legislation that would require entities that collect, sell, or use personally identifiable information (PII) through any medium to give consumers the opportunity to opt out from the sale of such information to third parties.

There would be no opt-out requirement for non-third party uses, but entities that offered opt-out opportunities for other uses of

the information would have to reveal that opportunity in their privacy statements, would have to make the opportunity "easy to access and to use," and would have to provide at least 30 days' notice "before materially changing the limitation [on use of the information] or terminating its compliance with the limitation."

The proposed Consumer Privacy Protection Act would require covered entities to notify consumers that their PII might be used for a purpose unrelated to the transaction in which it was collected and disclose any material change in the entity's privacy policy. Covered entities would also be required to establish a privacy policy on the collection, sale, and use of the consumer's information and make the policy easily accessible.

The bill would establish a safe harbor for entities that complied with a five-year self-regulatory program to be established by the Federal Trade Commission. The bill would create no private right of action and would preempt state and local privacy laws and enforcement of the federal law.

Rep. Stearns is a member of the House Energy and Commerce Committee's commerce, manufacturing, and trade subcommittee, which has jurisdiction over privacy matters. In the 109th Congress, he introduced privacy legislation that was not enacted, and he also worked on draft privacy legislation in the last Congress.

James Assey, executive vice president of the National Cable & Telecommunications Association said, "We applaud the efforts of Reps. Stearns and Matheson for adding their voices to the continued discussion about online privacy with the Consumer Privacy Protection Act of 2011."

"We particularly recognize the effort in this legislation to promote a level playing field with respect to privacy regulation," he added. "We look forward to further review of this bill and working with Reps. Stearns and Matheson, and other members of Congress as privacy legislation is considered this session."

Walter McCormick Jr., president and chief executive officer of the U.S. Telecom Association, also expressed support. "As an industry that already provides its customers with the highest levels of privacy protection, we especially appreciate Rep. Stearns' accompanying comments acknowledging that in today's converged communications marketplace, like services should be treated alike by the law and that a single agency should have this responsibility across the entire Internet economy," he said. -- Lynn Stanton, lynn.stanton@wolterskluwer.com

UTILITIES, REGULATORS WORKING ON CYBERSECURITY RELATIONSHIP

Federal government regulators and electric utilities are making some progress in establishing better relationships with each other over cybersecurity issues, but industry representatives indicated this week that more needed to be done to improve their cooperation.

Speaking at the Utilities Telecom Council's Smart Grid Policy Summit, Tim Roxey, director-risk assessment and technology division at the North American Electric Reliability Corp. (NERC), said NERC was working on "rules of engagement" with the Department of Homeland Security that he said would cut through some of the secrecy rules that prevent the government from sharing detailed security threat data with utilities. He said DHS was "getting better at understanding" electric grid security concerns, and had begun to pass along more relevant threat intelligence.

Mr. Roxey, whose duties include sending out threat alerts to utilities, said formulating those messages to optimize their usefulness was difficult given the vagueness of some threat data. "My team figures out what is actionable now," he said, adding, "there is hard, toe-to-toe" tussling above the top-secret level to distill threat data that can be filtered down to utilities.

He asked utility representatives to pay careful attention to the threat alerts. "Read every word, and think about why I wrote those words," he advised.

Robert McClanahan, vice president-information technology at Arkansas Electric Cooperative, urged the creation of incentives for better security performance by utilities. "We have to incent security instead of penalizing administrative errors," he said. "We have to get rid of the 'administrivia.' . . . We are a long way from that."

Mr. McClanahan said DHS had helped his company to get necessary clearances so it could attend higher-level threat meetings, but that it was up to the utility sector and the government to change the culture of trust between them. "We are going to have to learn how to act on less than a detailed description of an attack."

John Roukema, director-electric utility for Silicon Valley Power, echoed the need for better sharing of threat information. "At some point you have to share it and deal with it."

"We're not going to staff up to fight nation-states," Mr. Roxey said. But "some basic research" could make some of the more glaring electric utility security concerns go away, he asserted.

"We are not warfighters," Mr. McClanahan said. "We have an IT staff. . . . I'm not sure it's an electric cooperative's role to protect against a nation-state threat. That strikes me as a DoD [Department of Defense] role."

Mr. Roukema said it was the industry's obligation to know cybersecurity best practices. He suggested that security practices be standards-based and that vendors make sure that their products work for their intended security uses.

Similarly, Mr. McClanahan complained of what he called "a constant stream of changing regulations" for utility security, and the many regulators that can issue new ones, including the Federal Energy Regulatory Commission, the Department of Energy, DHS, and state regulators.

"I would like to lock them in a room, feed them nothing but coffee and bran muffins, and not let them out until they came up with one set of rules."

Also worrisome, Mr. Roxey said, is that increasing demands for electric utility cybersecurity may begin to outstrip the abilities of smaller utilities to handle them. He said there were more than 3,000 electric utilities in the U.S., including more than 2,000 municipal utilities. "Unfortunately, they are overtaxed," he said. "We can't keep up with the complexities. . . . The little people, I'm afraid, get crushed under it."

He added that smart grid systems as configured today might also lack adequate security. "My big fear is that with smart grid, we will do it wrong," he said. "We are relying on vendor specifications for [for smart meters] but within 10 years they will be found to be unsecure and will have to be replaced." -- John Curran, john.curran@wolterskluwer.com

DoJ TAKES AIM AT 'COREFLOOD' BOTNET WITH MIXTURE OF CIVIL, CRIMINAL TACTICS

The Justice Department this week used an unusual combination of civil and criminal authorities to seize control of an alleged botnet and replace one of the botnet's command-and-control servers with a substitute operated by the government.

The operation required the department, the U.S. attorney in Connecticut, and the Federal Bureau of Investigation to obtain warrants from criminal courts to authorize the seizure of five servers and 29 domain names while taking civil action in U.S. District Court for the District of Connecticut to deploy the substitute server.

The new server is key to permanently disabling the "Coreflood" botnet, the department told the court in an April 12 filing. "The seizures will break the [botnet operators'] hold over the infected computers for a time, but will leave hundreds of thousands of infected computers that are still running Coreflood, still surreptitiously collecting private personal and financial data, and still 'beaconing' to the Internet for further instructions," it said.

That would enable the botnet's operators, identified in court documents as 13 "John Does," to regain control of the botnet, DoJ said. Instead, a substitute server "operated under law enforcement supervision by the nonprofit Internet Systems Consortium" will order the Coreflood malware to shut down on infected computers. That will give the owners of infected machines a chance to purge the virus.

"This is the first case in which United States law enforcement authorities have requested authorization to control a seized botnet using a substitute command-and-control server," DoJ noted. Last year, Dutch authorities took a similar step in an effort to disable the BredoLab botnet.

The transnational nature of cyber crime, the anonymity of the Internet, the resilience of botnets, and limits on DoJ's authority have fueled a surge in botnet-enabled cyber crime. Microsoft Corp. has used civil lawsuits to try to disable two botnets -- most recently the Rustock botnet (CPR, March 21).

The Justice Department, meanwhile, has relied on criminal investigations, which can be ineffective against overseas defendants. At a hearing this week, Sen. Sheldon Whitehouse (D., R.I.) cited Microsoft's success and pointedly asked officials from DoJ and the FBI to consider adding civil injunctive relief to their cyber crime toolbox.

Although a federal judge granted DoJ's request to deploy the substitute server, Justice Department attorneys had to jump through some hoops. First, they filed their petition in Connecticut, which they decided had a state law that would favor their request, and they cited case law that suggested that federal courts should apply some state laws when its jurisdiction is unclear.

Second, they convinced the judge that the botnet's operators, who are thought to live overseas, could receive adequate notification of the action against them by posting court documents on the Internet and sending those documents to the postal and e-mail addresses they provided to their domain name registrars.

DoJ also went to great lengths to argue that automatically shutting down the Coreflood virus on individual computers did not amount to an unconstitutional intrusion onto personal turf. "It is very likely that the owners of the infected computers will not even

notice that the Coreflood software has stopped running, as they are very likely unaware of it to begin with," DoJ attorneys argued.

"Instead, in a sense, the government is mitigating what amounts to be a public nuisance, one that threatens the privacy and security of the owner of an infected computer, but also others who may use the infected computer or whose computers may become infected with Coreflood," they said.

"The owner of an infected computer who wants Coreflood to continue running on an infected computer need only create a file on the infected computer that overrides the DNS [domain name system] lookup for the Coreflood domains," they said.

Coreflood has infected more than 2 million computers worldwide, and its operators have used it to steal an unknown amount of money from businesses and consumers, DoJ alleged. Its victims, DoJ said, include a real estate company in Michigan, which had $115,771 stolen from its bank account; a South Carolina law firm that lost $78,421; and a Tennessee defense contractor that had $241,866 stolen.

"Due to the sheer volume of data and the difficulty identifying victims, it has not been possible to determine the full extent of the fraud losses attributable to the Coreflood botnet," the department told the court.

The department indicated it would seek a civil restraining order that would permanently deprive the botnet's operators of their servers and domain names and, on the criminal side, attempt to capture and convict the operators. -- Tom Leithauser, tom.leithauser@wolterskluwer.com

OBAMA DIRECTS AGENCIES TO PREPARE FOR CYBER ATTACKS, OTHER DISASTERS

The White House has issued instructions to its homeland security adviser, John Brennan, to coordinate interagency development and an implementation plan for a national preparedness system that would respond to major disasters including cyber attacks. Homeland Security Secretary Janet Napolitano will be in charge of the much of the plan development.

According to a presidential policy directive dated March 30 and obtained by the "National Journal," the directive is aimed at "strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters."

While the White House directive says it is "intended to galvanize action by the federal government," it also says that the private and nonprofit sectors and private citizens also share responsibility for preparedness and should assist in "an integrated, all-of-nation, capabilities-based approach to preparedness."

The White House wants to come up with a preparedness goal that identifies core capabilities and a national preparedness system "to guide activities that will allow the nation to achieve the goal."

Mr. Brennan, assistant to the president for homeland security and counterterrorism, has been instructed to coordinate interagency development and give President Obama an implementation plan within 60 days of March 30. The plan will assign departmental responsibilities and delivery timelines for "for the development of the national planning frameworks and associated interagency operational plans," the directive says.

Homeland Security Secretary Janet Napolitano is tasked with developing and delivering the national preparedness goal within 180 days and consulting with federal agencies, state, local, tribal, and territorial governments, the private and nonprofit sectors, and the public.

The goal document will be "informed by the risk of specific threats and vulnerabilities," and "include concrete, measurable, and prioritized objectives to mitigate that risk," the directive says.

The DHS chief will have 240 days to deliver a national preparedness system document to the president, with work on that also to be coordinated with the same variety of government agencies and the private and nonprofit sectors.

The system document will include "guidance for planning, organization, equipment, training, and exercises to build and maintain domestic capabilities," and to "sustain a cycle of preparedness over time." The national preparedness system will include provisions for sharing personnel and equipment guidance "aimed at nationwide interoperability."

Within one year, the DHS chief will submit to the White House the first annual national preparedness report. -- John Curran, john.curran@wolterskluwer.com

U.S., EU PLEDGE TO DEEPEN CYBERSECURITY PARTNERSHIP

U.S. and European officials this week "reiterated their shared commitment to deepening cooperation" to address cyber crime. At the April 14 EU-U.S. Justice and Home Affairs Ministerial in Hungary, the two sides "agreed to strengthen trans-Atlantic cooperation in cybersecurity by defining the issues to be tackled" by a joint working group on cybersecurity and cyber crime. Among other things, the working group intends to conduct an EU-U.S. cyber exercise by year-end.

EGYPT TO REVIEW LAW ALLOWING OFFICIALS TO DISABLE INTERNET

The decision to disable Internet and mobile communications during the Egyptian revolution was "inappropriate," and the law used "by the previous regime" to justify the action will be examined, the Egyptian Cabinet of Ministers announced. A provision of the country's communications law "stipulates that proper authorities of the land can instruct service providers and mobile operators to cut their services in the case of any disaster or situation jeopardizing the national security of the country," the cabinet noted. But the cabinet is preparing an amendment that would "prohibit any entity from unilaterally cutting communications and Internet," said Magued Osman, Minister of Communications and Information Technology. "The communications and Internet cut will not happen again."