



WARREN'S Washington Internet Daily

Covering Legislative, Regulatory and Judicial News Affecting Internet Business. From the Publishers of **Communications Daily**.

TUESDAY, MAY 31, 2011

VOL. 12, NO. 104

Today's News

IDENTITY OF HACKER still unknown, but Sony believes breaches of PSN, SOE services were 'perpetrated by the same person,' it says. (P. 1)

PATRIOT ACT EXTENSION of roving wiretap, national security letter powers signed into law moments before deadline. (P. 2)

SMART TV PRIVACY RULES unclear to some, problematic for others. (P. 4)

COURTS: PayPal, eBay sue Google over mobile Wallet product, claiming trade-secrets violation. (P. 5)

INTERNATIONAL: EC to hold meeting to assess the progress of Europe's digital agenda. (P. 6)

INDUSTRY NOTES: Travelport deploys Cisco data center technology ... Shoppers interact regularly with retailers on social network sites, Shop.org study says. (P. 6)

Identity of Hacker Still Unknown, Sony Says in Letter

Sony has "not yet identified" the hacker or hackers who breached its Sony Network Entertainment America (SNEA) and Sony Online Entertainment (SOE) services, Sony Computer Entertainment America (SCEA) Chairman Kazuo Hirai said in a letter to House Commerce Manufacturing Subcommittee Chairwoman Mary Bono Mack, R-Calif., and ranking member G.K. Butterfield, D-N.C. But Hirai said "the timing, techniques, and methods used by the hacker suggest that the SOE breach was perpetrated by the same person or persons as" the PlayStation Network (PSN) breach. SNEA includes Sony's PSN and Qriocity music services.

The letter was in response to lingering questions that the subcommittee had after Hirai discussed the breaches in a letter to the subcommittee last month (WID May 5 p1). It received Hirai's latest letter Thursday evening and made it available Friday.

Mack had said she wasn't satisfied with Sony's reasons for not notifying its customers about the breaches sooner. She "remains critical of Sony's initial handling of the data breaches," Mack spokesman Ken Johnson said Friday. Mack was "satisfied that Sony made a good faith effort to answer our questions," but Hirai shed no new light in his latest letter on why Sony didn't inform consumers about the breaches earlier, Johnson told us by phone on Friday. The answers "lacked depth," he said.

But Johnson said Mack was "appreciative that Sony has now agreed to testify" at the next data security hearing of the subcommittee, June 2. "Hopefully, we'll find out more in our hearing," he told us, saying Mack planned to explore the timing of Sony's response to consumers in more depth. Tim Schaff, president of Sony Network Entertainment International (SNEI), is expected to represent Sony at the hearing, Johnson said. Mack "firmly believes that the lessons learned from both the Sony and Epsilon experiences can be instructive and guide us as we develop comprehensive data protection legislation," Johnson said. "We expect to introduce that legislation, which will provide new safeguards for American consum-

ers, in the next few weeks," he said. A requirement to promptly inform consumers about such breaches will be a key component of the legislation, he told us.

Sony has "information that suggests what the hacker was accessing and what the hacker may have downloaded, but we are unable to determine conclusively whether information was actually taken from all or just a portion of the user accounts," Hirai said in the Thursday letter. Therefore, the company believed it was "appropriate for notification purposes to assume information could have been taken from any of the 77 million" SNEA accounts, he said. Based on evidence that was available to Sony on May 3, it "believed that no credit card data had been taken from PSN/Qriocity but could not rule it out," he said. Since then, he said, "no further forensic or circumstantial evidence has been discovered to suggest that any credit card data was taken." There also had, to date, "been no confirmed reports of credit card misuse or reports of an increase in fraudulent transactions resulting from this incident," he said.

The company also thinks it knows "how the hacker gained access to each of the two networks, but the investigation is ongoing regarding other aspects of the criminal attack," Hirai said. Sony believes that "publicly releasing these facts could jeopardize the ongoing investigation and potentially put other network systems at risk," he said. Hirai offered "to explore a confidential and secure manner in which to outline this information to" the subcommittee.

Separately, Sony Corp. and Sony Computer Entertainment said Friday that SNEI planned, the next day, to start "a phased restoration of" PSN and Qriocity services in Japan and other Asian countries and regions including Taiwan, Singapore, Malaysia, Indonesia and Thailand. As in North America and Europe, a new identity protection program would be offered in conjunction with the phased restoration for PSN and Qriocity customers in Japan, Sony said. Sony was "working closely with respected outside security firms," and "implemented new and additional security measures that strengthen safeguards against unauthorized activity, and provide consumers with greater protection of their personal information," it said. A chief information security officer was also created at SNEI who "will work to reinforce overall information security across the company's network infrastructure," it said. The first phase of restored services for the Asian countries and regions will include a "Welcome Back" package of services and premium content to all registered customers, as in North America and Europe, it said. The details of the program "will be announced in each" Asian "region shortly," it said. Last week, SCEA said PSN and Qriocity account holders in the U.S. could start the enrollment process for the new identity theft protection program after the recent restoration of services there. — *Jeff Berman*

EFF: Fight Not Over

Obama Signs Renewal of Government Spying Powers

The government may continue using roving wiretaps and other Patriot Act powers that were to expire at 12:01 a.m. Friday. Late Thursday, President Barack Obama signed into law an extension until June

By using our e-mail delivery service, you understand and agree that we may use tracking software to ensure accurate electronic delivery and copyright compliance. This software forwards to us certain technical data and newsletter usage information from any computer that opens this e-mail. We do not share this information with anyone outside our company, nor do we use it for any commercial purpose. For more information about our data collection practices, please see our Privacy Policy at www.warren-news.com/privacypolicy.htm.

1, 2015, of the government spying powers. The law made no changes to surveillance, but Senate Judiciary Committee Chairman Patrick Leahy, D-Vt., introduced legislation Thursday based on his failed amendment to add privacy protections. House Minority Leader Nancy Pelosi, D-Calif., and privacy groups said they were disappointed the renewal had no new protections for U.S. citizens.

The renewed Patriot Act sections relate to roving wiretaps allowing the government to continue tracking a suspect who switches phones under the same warrant, Section 215 orders to obtain "any tangible thing," and "lone wolf" attacks. Sen. Rand Paul, a tea party Republican from Kentucky, slowed movement through Congress with a plethora of amendments, but early Thursday evening the Senate passed the bill 72-23. A few hours later, the House concurred by a vote of 250-153. Obama signed the bill Thursday night, the White House said a few minutes before midnight.

"Although the PATRIOT Act is not a perfect law, it provides our intelligence and law enforcement communities with crucial tools to keep America safe and thwart terrorism," Senate Majority Leader Harry Reid, D-Nev., said in a written statement. "While I am disappointed we were not able to include any of the sensible oversight and civil liberties protections included in the bill reported by the Judiciary Committee with bipartisan support, I strongly support the Senate's effort to ensure that these important authorities do not expire." Minority Leader Mitch McConnell, R-Ky., said "the invaluable terror-fighting tools under the Patriot Act have kept us safe for nearly a decade, and Americans today should be relieved and reassured to know that these programs will continue."

But Pelosi complained about the bill's lack of privacy protections. "Congress failed to seize the opportunity to enact measures and improvements needed to preserve Americans' privacy and to incorporate oversight and compliance with the law," Pelosi said in a statement. "In addition, Congress failed to consider meaningful reforms to National Security Letters to address documented abuses. Instead, we were left to vote only on a long extension of some of the most controversial and troubling aspects of the PATRIOT Act."

Leahy, whose amendment was rebuked in the Senate by McConnell, promptly reissued his proposed reforms in a new free-standing bill, S-1225. The bill makes changes to the Foreign Intelligence Surveillance Act to bolster people's privacy.

While disappointed that the renewal contained no new protections, the Electronic Frontier Foundation was happy to see more members voting no on the Patriot Act extension, said EFF Senior Staff Attorney Kevin Bankston in an interview. Patriot Act opponents picked up 12 additional no votes in the Senate and 10 in the House, compared to the last time renewal was raised, Bankston said. That includes not only Democrats, but several tea party Republicans, he said. Congress shouldn't let a Patriot Act re-vamp stagnate for another four years, he said. EFF supports Leahy's new bill, though it would prefer even stronger changes to surveillance law, Bankston said: "The renewal fight may be over, but the fight for reform will continue."

"Despite having months to debate and legislate on this crucial issue, Congress has once again chosen to rubberstamp the Patriot Act and its overreaching provisions," Linda Murphy, Washington director of the American Civil Liberties Union, said in a statement. "Since its passage nearly a decade ago, the Patriot Act has been used improperly again and again by law enforcement to invade Americans' privacy and violate their constitutional rights." — *Adam Bender*

TV Privacy

Privacy Framework for Smart TV Sets, Services Not Clear Cut

The privacy rules covering so-called “smart TV” services and devices aren’t clear, industry executives and public interest advocates said. That could be a problem if such services become popular with consumers, as TV set makers and pay-TV distributors seek to add apps, widgets, interactivity and ad targeting to their services, they said. “The same business models that collect a tremendous amount of data online, and have raised privacy concerns in congress and at the FTC, can now be found on the television set,” said Jeff Chester, executive director for the Center for Digital Democracy. “This is a major privacy issue that is about to boil over and regulators will be caught flat footed by not trying to address it,” he said.

A variety of laws and regulations cover privacy on the TV set, industry lawyers said. The Children’s Online Privacy Protection Act (COPPA) address’s children’s privacy for all Internet services and the Cable act has provisions that address privacy for pay-TV services, they said. “If someone is an MVPD under the Cable Act, then everything they touch is subject to the protections of the act,” said Paul Glist, an attorney with Davis Wright who represents cable operators. “But if someone comes in and builds a smart TV with set-top-box-like functionality, they’re not considered a cable operator and they’re not considered a satellite provider,” he said.

“It really is the classic unanswered question,” said Marcelino Ford-Levine, general manager, interactive content and advanced advertising development, for Intel’s Digital Home Group, at a recent interactive TV conference in San Francisco. “We’ve been looking at the privacy issues and trying to understand how to pass what we see emerging as a bright line test,” he said. “You really have to educate the consumer as to what their data is going to be used for” and give them the ability to opt in, and “at any time press the delete button and say ‘I want out,’” he said. “It’s really going in that direction.”

Existing safeguards are inadequate, Chester said. “If it’s connected to the Internet, then you do have COPPA but you have nothing else to the extent to which they’re able to collect data about your online activity through the TV set,” he said. “That’s a gray area,” he said. But it might not be completely gray, at least for third-party devices that allow access to traditional pay-TV service. The Cable Act protections can be applied to those devices through a license and contract system between pay-TV service providers and device manufacturers that guarantee the integrity of the customer experience, including privacy, Glist said. “There is actually a customer relationship there that needs to be assured, and privacy is an element of that,” he said. “You can do it through B-to-B agreements, or generally applicable licenses,” he said. “You can do it by a rider on the decryption licenses,” he said.

The pay-TV providers’ advanced ad plans should raise privacy concerns, Chester said. “They have the majority of eyeballs and they have access to the real financial records,” he said. “They’re creating a wide range of data collection practices that fly in the face of any notion of privacy.” — *Josh Wein*

Capitol Hill

A bipartisan majority of House members support wireless tax legislation by Rep. Zoe Lofgren, D-Calif. The bill, which would ban for five year states from taxing wireless goods and services, secured its

218th cosponsor on Thursday. A similar bill in the Senate by Sen. Ron Wyden, D-Ore., has seven cosponsors not counting John Ensign, R-Nev., who has since resigned. Markup of the bill by the full House Judiciary Committee is expected soon, a House aide said. — **AB**

The House Oversight Committee announced a cybersecurity hearing for Wednesday. The hearing “will assess the federal government's efforts, including current and proposed Obama Administration policy, to improve the Nation's resilience to the growing cybersecurity threat,” the committee said. The full committee hearing comes one week after a National Security subcommittee hearing on the threat of cyberattacks (WID May 26 p4). The hearing is at 9:30 a.m. in Room 2154, Rayburn House Office Building.

Courts

Google poached top executives from PayPal and parent company eBay who were in charge of mobile payments before announcing its Wallet service last week, the companies alleged in a trade-secret lawsuit against Google filed in California Superior Court in Santa Clara County. Google Wallet relies on a near-field communication chip that will be included in future Android phones that can be used for purchases on some point-of-sale terminals. Osama Bedier worked for PayPal from December 2002 to Jan. 24, 2011, departing as vice president of platform, mobile and new ventures and joining Google, the suit said. Stephanie Tilenius, eBay senior vice president of North America and global products when she left in 2009, came back to eBay under a consulting agreement that ended March 3, 2010 — but she joined Google as vice president of electronic commerce on Feb. 16 of that year, the suit said. PayPal and eBay also filed against people who they believe are 50 unknown defendants who were involved in the executives' move to Google. Bedier had "intimate knowledge" of PayPal's mobile payment strategy and capabilities that he disclosed to Google and "major retailers" when he left PayPal, the suit alleged. Tilenius recruited Bedier to Google, violating her "contractual obligations" to former employer eBay. Crucially, Google and PayPal were negotiating a deal between 2008 and 2011, led by Bedier, in which PayPal would be a payment option for mobile purchases on the Android Market: "During that time, PayPal provided Google with an extensive education in mobile payments." Bedier was interviewing for the Google job "at the very point" when Google and PayPal were finalizing the deal, the suit said, conduct which "amounted to a breach of his responsibilities" at PayPal. The suit alleged that Bedier transferred "up-to-date versions of documents" on PayPal's mobile payment and point-of-sale strategies to his "non-PayPal computer just days before leaving PayPal" for Google: "On information and belief," Bedier had already decided to join Google and "had no legitimate reason for obtaining an update on PayPal's strategies." Bedier also has refused PayPal attempts to secure the "proper return and analysis of its trade secret information" from his computers, email and online storage accounts, the suit claimed. The executives' move was especially worrisome because of Google's failure to tap the mobile-payments market through its Checkout system, which is "mostly a tool for acquiring customer information for the benefit of Google's other products and services" and whose revenue Google reported as "not material" in its 2010 annual report, the suit said. Yet with 30 percent of the smartphone operating system market, Google can leverage that base to get an "early adoption" advantage with retailers and consumers. Despite the "relatively recent" use of smartphones for point-of-sale transactions, "PayPal's trade secrets are particularly valuable in this emerging area," the suit said. Both companies are doing mobile-payment trial runs with major retailers, and it's "unlikely that a retailer would invest time and effort in testing both companies' products." A Google spokesman said the company respects trade secrets and will defend itself. "Silicon Valley was built on the ability of individuals to use their knowledge and expertise to seek better employment opportunities, an idea recognized by both California law and public policy," he said.

International

The European Commission will gauge the progress of Europe's digital agenda at a June 16-17 meeting in Brussels, it said Friday. Participants at the first "digital agenda assembly" include representatives from industry, the research community, nongovernmental organizations, governments and other EU bodies, it said. There will be workshops on key topics such as high-speed broadband rollout, cybersecurity, child online safety, radio spectrum for wireless services and cloud computing, it said.

Industry Notes

Travelport selected Cisco's infrastructure platform "to increase business agility, scalability and efficiency for its primary data center," Cisco said. Travelport provides transaction services for several countries and travel agencies. With Cisco data center technology, Travelport can add data center capacity "at a rapid rate without having to add information technology staff," Cisco said.

Shoppers are willing to interact with retailers through Facebook, Twitter or a blog, said a joint study by ComScore, Shop.org and Social Shopping Labs. More than 1,700 adult online shoppers were polled in April for the 2011 Social Commerce Study, Shop.org said. Nearly 60 percent of respondents said they follow companies online to find deals, the study said. About 50 percent follow companies "to keep up to date on products," while 39 percent connect with retailers online for contests and events information, Shop.org said. Some shoppers, 35 percent, said they would be likely to make purchases directly from Facebook, and 32 percent from Twitter, the report said. About 57 percent of consumers who use group-buying sites like Groupon and Gilt City, "spent over \$100 through these sites to date."

Internet People

Presidential appointees to National Security Telecom Advisory Committee: **Scott Charney**, Microsoft; **Dick Costolo**, Twitter; **David DeWalt**, McAfee; **Jamie Dos Santos**, Terremark; **Lisa Hook**, Neustar.

Washington Internet Daily Calendar

- June 1 Information Technology & Innovation Foundation panel on government broadband subsidies, 9 a.m., 1101 K St. NW, Washington — www.itif.org
- June 1 Heritage Foundation panel on Internet Freedom in Russia, 11 a.m., 214 Massachusetts Ave. NE, Washington — 202-675-1761
- June 1 Cisco releases findings of global broadband survey, noon, National Press Club, Washington — 202-463-0013
- June 2 USTelecom webinar on IPv6 and telecom networks, 1 p.m. — webinars@ustelecomwebinars.com
- June 2-3 Copyright Office public meeting on pre-1972 sound recordings, 9 a.m., Library of Congress, Washington

- June 7 FCBA CLE on emerging video platforms, 6 p.m., Davis Wright, 1919 Pennsylvania Ave. NW, Washington — www.fcba.org
- June 7-8 International Confederation of Societies of Authors and Composers, World Copyright Summit, Square Brussels Meeting Center, Brussels — www.copyrightsummit.com
- June 9 FCC meeting, 10:30 a.m., Commission Meeting Room — www.fcc.gov
- June 9-10 HB Litigation Conferences cyberrisk and privacy liability seminar, Union League, Philadelphia — www.litigationconferences.com
- June 10 FCC Emergency Access Advisory Committee meeting, 10:30 a.m., Commission Meeting Room — 202-418-2284
- June 10 FCBA annual lunch with FCC Chairman Julius Genachowski, noon, Capitol Hilton, Washington — fcbaevents@fcba.org
- June 10 Copyright Office public hearing on statutory licensing, Room LM-408, Madison Building, Library of Congress — <http://xrl.us/bj4iun>
- June 14-15 Mobile Venture Summit, Fox Theatre, Redwood City, Calif. — tp@aonetwork.com
- June 27-28 Legal IQ forum on e-discovery, location TBA — info@iqpc.com
- June 27-29 Emerging Communications Conference, San Francisco Airport Marriott — <http://ecommerce.com>
- July 12 FCC meeting, 10:30 a.m., Commission Meeting Room — www.fcc.gov



(ISSN 1530-0501)

PUBLISHED BY WARREN COMMUNICATIONS NEWS, INC.

Michael Feazel Managing Editor
 Dugie Standeford European Correspondent
 Scott Billquist Geneva Correspondent

Warren Communications News, Inc. is publisher of Communications Daily, Warren's Washington Internet Daily, Consumer Electronics Daily, Green Electronics Daily, Washington Telecom Newswire, Telecom A.M., Television & Cable Factbook, Cable & Station Coverage Atlas, Public Broadcasting Report, Satellite Week and other special publications.

Send news materials to: newsroom@warren-news.com

Copyright © 2011 by Warren Communications News, Inc.
 Reproduction in any form, without written permission, is prohibited.

EDITORIAL & BUSINESS HEADQUARTERS
 2115 Ward Court, N.W., Washington, DC 20037
 Phone: 202-872-9200 Fax: 202-318-8984
www.warren-news.com
 E-mail: info@warren-news.com

WASHINGTON HEADQUARTERS

Albert Warren
Editor & Publisher 1961-2006

Paul Warren Chairman and Publisher
 Daniel Warren President and Editor
 Michael Feazel Executive Editor
 Howard Buskirk Senior Editor
 Dinesh Kumar Senior Editor
 Jonathan Make Senior Editor
 Adam Bender Associate Editor
 Bill Myers Associate Editor
 Yu-Ting Wang Assistant Editor
 Tim Warren Assistant Editor
 Kamala Lane Assistant Editor
 Bryce Baschuk Assistant Editor

Louis Trager Consulting News Editor
 Josh Wein West Coast Correspondent
 Greg Piper Seattle Correspondent

Television & Cable Factbook

Michael Taliaferro Managing Editor
 Gaye Nail Assoc. Managing Editor
 Kari Danner Sr. Editor & Editorial Supervisor
 Colleen Crosby Sr. Editor & Editorial Supervisor
 Bob Dwyer Senior Research Editor
 Marla Shepard Senior Editor

Business

Brig Easley Exec. VP-Controller
 Deborah Jacobs Information Systems Manager
 Gregory Jones Database/Network Manager
 Gina Storr Director of Sales & Marketing Support
 Annette Munroe Asst. Dir., Sales & Mktg. Support
 Susan Seiler Content Compliance Specialist
 Katrina McCray Sr. Sales & Mktg. Support Specialist
 Greg Robinson Sales & Marketing Support Assistant
 Loraine Taylor Sales & Marketing Support Assistant

Sales

William R. Benton Sales Director
 Agnes Mannarelli National Accounts Manager
 Jim Sharp Account Manager
 Brooke Mowry Account Manager
 Norlie Lin Account Manager

NEW YORK BUREAU

276 Fifth Ave., Suite 1002, N.Y., N.Y. 10001
 Phone: 212-686-5410
 Fax: 212-889-5097

Paul Gluckman Bureau Chief
 Mark Seavy Senior Editor
 Jeff Berman Senior Editor
 Rebecca Day Senior Editor
 Razia Mahadeo Editorial Asst.
 Barry Fox Contributing Editor

By using our e-mail delivery service, you understand and agree that we may use tracking software to ensure accurate electronic delivery and copyright compliance. This software forwards to us certain technical data and newsletter usage information from any computer that opens this e-mail. We do not share this information with anyone outside the company, nor do we use it for any commercial purpose. For more information about our data collection practices, please see our Privacy Policy at www.warren-news.com/privacypolicy.htm.