WARREN COMMUNICATIONS NEWS Telecom & Media Intelligence www.warren-news.com

WARREN'S Washington Internet Daily

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

FRIDAY, JUNE 8, 2012

VOL. 13, NO. 111

Today's News

GET GOING ON IPv6, Cerf says. Enabling IPv6 for Internet of Things could be next step, major players say. (P. 1)

CISPA COMPROMISE SOUGHT by lawyer for originating House committee. (P. 3)

ITU INTERNET REGULATION effort can be advanced by Dubai conference in December even if onerous treaty isn't direct outcome, warns CCIA's Black. (P. 4)

BACKPAGE.COM SECURES temporary restraining order against Washington sex-ad law it claims violates CDA. (P. 4)

CAP DRAWS WEB INTEREST, as sites seek alert feed that's going online, FEMA, industry officials say. (P. 6)

PATENT-BASED EXCLUSIONS of imports of IT and telecom products can harm competition and consumers, FTC says. (P. 7)

CAPITOL HILL: House and Senate Intelligence leaders call for investigation into alleged cybersecurity leaks ... Bipartisan national security experts back critical-infrastructure regulation in cyberbills. (P. 9)

Successful IPv6 Launch Could Pave the Way for Use in Internet of Things

IPv6 has been "proven ready for business" after more than 3,000 websites, 60 access providers and five home router vendors moved permanently to it for the Internet Society world launch Wednesday, ISOC Chief Internet Technology Officer Leslie Daigle told a news briefing Thursday. "There are no more excuses" for not running IPv6 alongside IPv4, said Google Internet Evangelist Vint Cerf. Companies that aren't capable of doing so must "get going," he said. While it will take time for the technology to spread to all networks, websites and consumer equipment, some players are already looking ahead to its uses in emerging technologies such as the Internet of Things (IoT), smart grids and cloud computing, they said. There's a much larger supply of IPv6 addresses, vs. a dwindling supply of IPv4 Internet Protocol addresses.

The launch brought "24 hours of seamless deployment" and "24 hours of 0 impact, 0 cases" of problems attributable to turning on IPv6, Cisco Fellow Mark Townsley said. The company saw much more traffic moving on the new version than beforehand, he said. Google has seen a 70 percent increase in Web traffic over IPv6 since Wednesday, said Ipv6 Software Engineer Erik Kline. However, there wasn't a dramatic increase in high-bandwidth traffic because YouTube videos have been available on IPv6 since last June, he said. More than 27 million active Facebook users now have IPv6 in their homes, a number 3-5 times higher than 12 months ago, said Senior Network Engineer Donn Lee.

Asked what's being done to encourage additional content providers to make content available over IPv6, Daigle said that along with the many website operators participating in the transition, there are also content delivery networks such as Akamai and hosting companies such as Dreamhost making it easier for smaller websites to

Copyright© 2012 by Warren Communications News, Inc. Reproduction or retransmission in any form, without written permission, is a violation of Federal Statute (17 USC01 et seq.).

turn on IPv6. The technology has been around for some time, and people are gradually making it part of their normal business operations, she said. The global launch may impel other websites to do what they need to do, she said.

"Public embarrassment may be our friend here," Cerf said. Some organizations may be shamed into taking up IPv6 alongside IPv4, he said. As equipment moves to the new version, providers will have to as well, he said. Some companies have enabled IPv6 quietly, the way Wikipedia did, said Alain Fiocco, a Cisco senior director. Many more enterprises, such as banks, will do the same, he said. The transition should be absolutely transparent to users, Cerf said.

Now that the big Internet industry is behind IPv6 to "fix the nitty-gritties," it's time to pursue other critical work in enabling the technology in the IoT, smart grids, cloud computing, smart cities, and other areas, IPv6 Forum President Latif Ladid told us. "The restoration of the end-to-end model is going to be a key innovation driver."

The smart grid program has adopted IPv6 as the preferred way of providing the large number of addresses needed for many devices, Cerf told the briefing. Mobile operators in the Third Generation Partnership Project also say they prefer IPv6, he said. But it's vitally important that both protocols be able to run at the same time, he said, because if they don't, website hyperlinks might not work.

Comcast views IPv6 as an enabler of the IoT, said John Brzozowski, chief architect for IPv6. The cable ISP hopes to embark on some innovations in this area, he said. Although proponents of the new protocol originally pushed people to adopt it because of the depletion of IPv4 addresses, the launch should catalyze other innovations, he said.

A large part of ISOC's interest in IPv6 has to do with enabling the future Internet, Daigle said. It was important to show that the protocol is real so people can continue to build the Internet as a platform for new products and services, she said. IPv6 offers the potential to avoid network translation, allowing machines to talk directly to each other, Cerf said. It will spur growth of networks of sensing, monitoring, and access and control systems, he said.

The launch was just the beginning, several speakers said. It will give companies the chance to learn more about how the networks function and how people use the protocol, said Microsoft Bing Program Manager Kevin Boske. The global rollout was a "running start," said Townsley. It only takes one leader to step forward for others to fall in behind, he said. Cerf said he wants the Internet fully operational via IPv6 no later than 2015.

Preliminary data shows that the launch "was not simply turned on with one big flick of a switch" but merely served as a deadline that many websites have been working toward over the past year, Sandvine Chief Technology Officer Don Bowman wrote Thursday on the ISP vendor's blog (http://xrl.us/bna5uk). While there was a noticeable uptick in traffic June 6, the majority of it came from Netflix and YouTube, he said. The latter accounted for more than half of all native IPv6 traffic in the U.S., while Facebook "leapt up the list," he said. Netflix, rolling out IPv6 coverage over the last few weeks, moved to second on the list, he said.

By Wednesday evening, the Amsterdam Internet Exchange had witnessed an increase of 1.2 Gbps via IPv6 traffic compared to previous days, Incognito Software Chief Technical Officer Chris Busch told us. That shows that the ability of Web traffic to natively traverse the Web within the new protocol is al-

ready making an impact, he said Wednesday. Considering that the exchange also showed total traffic at around 1.4 Tbps, "this actually illustrates just how far of a journey remains for the worldwide implementation of IPv6," he said. Incognito supplies broadband software provisioning products, while Sandvine's products are used by ISPs to manage traffic.

The biggest issue for the industry will be "caused by the consumer electronics space," Busch said. While newer operating systems in laptops and computers support the protocol natively, many consumer devices still tend to favor the earlier version, he said. "It may actually be the slow course of IPv6 transition mechanisms that ultimately pushes customer adoption" toward devices with native IPv6 support, he said. Some applications and services don't work well when translated between IPv6 and IPv4, causing them to break or stop operating, he said. That "application brokenness" at the customer and end-consumer level is likely to be the real driver of IPv6 adoption and could also force a higher percentage of IPv6 native traffic across the rest of the Internet, he said. — ***Dugie Standeford***

Waiting for Senate

Pro-CISPA Committee Aide Solicits Compromise, but Intel, Libertarian Representatives Say It Won't Come

NAPA, Calif. — CISPA's sponsors are ready to talk turkey if the Senate can muster an alternative bill, though they have dealt with legitimate qualms and remaining objections are baseless, said an aide to the committee that produced the Cyber Intelligence Sharing and Protection Act. "It's hard for us to read the tea leaves on this," but "we're hopeful the Senate passes something," Jamil Jaffer, senior counsel to the House Intelligence Committee, said late Wednesday. "We're ready to go to conference and find a middle ground. ... We're hoping to get to a deal that gets information security in some way, shape or form, whatever that looks like," he said at the Tech Policy Summit.

Representatives of Intel and a business think tank said no deal seems to be in the cards. "It's going to be difficult to get agreement" about who is to regulate what regarding critical infrastructure and even what that term means in the context, said Audrey Plonk, a security and Internet policy specialist at Intel. The telecom and IT industries are reluctant to submit to regulation by the Department of Homeland Security as proposed in the Cybersecurity Act (S-2105) by Sens. Joe Lieberman, I-Conn., and Susan Collins, R-Maine, which the administration has gotten behind, Plonk said. "Legislation that goes in that direction I think is a non-starter," she said. Though "a lot of the groups that opposed [the Stop Online Piracy Act] are on board with this," legislation along these lines is too contentious to "go anywhere in the Senate this year," said Wayne Crews, the Competitive Enterprise Institute's policy vice president.

"You can do an easier bill" by narrowing the goals to encouraging the government to share cybersecurity information with businesses and to giving companies an antitrust exemption for sharing the information among themselves, Crews said. Deregulating critical infrastructure would "make it more resilient," helping the owners "block any particular attack," he said.

Crews sought to position CISPA as a step in a police-state trend extending back to Total Information Awareness (TIA), a George W. Bush administration data-mining initiative, and forward to more ominous measures. The bill would allow companies to ignore privacy promises to customers in sharing cyber information, he said. Jaffer called the comparison to TIA "a canard" and said it was "ridiculous and false"

to contend that the bill's "notwithstanding any other provision of law" immunity for companies would "trump private contracts" with users. — ***Louis Trager***

WCIT in Dubai

Regulatory Threat to Internet Through ITU Treaty Said to Extend Well Beyond December Conference

NAPA, Calif. — A December ITU conference could lay the groundwork for far-reaching regulation of the Internet by treaty, though it probably won't be any "absolute catastrophe" in its concrete results, said Ed Black, Computer & Communications Industry Association president, Thursday. The one-country, one-vote World Conference on International Telecommunications in Dubai takes international pro-regulatory discussions of recent years "to a whole new level" because it's dealing with proposals for binding obligations, said Sally Wentworth, Internet Society senior manager-public policy. They spoke at the Tech Policy Summit.

Efforts to regulate reflect a recognition by governments of the Internet's ability "to disrupt existing power structures, business models, governmental control," Black said. "Conscious and willful" work by governments such as those of Russia and China to extend online the kind of control they exert over their societies are compounded by others' well-meaning or innocuous-sounding efforts to achieve "social goals" with "careless disregard of the consequences" of fettering cyberspace, he said. Ghana's, for instance, involves green energy, Black said.

Some officials, like those in French-speaking Africa, have gotten the misimpression that the best way to finance broadband networks is by imposing telecom style per-minute billing for Internet use, said Robert Pepper, Cisco vice president-technology policy. "There are countries that want to make ... technical standards binding," he said. "Think how restrictive that would be." If this came to pass, "you'd probably send lawyers" to meetings of standards-setting bodies, "because you're developing something that would be an obligation," Wentworth said. Other proposals involve information security and spam, she said. "One country's spam is another country's free speech." To be broad enough to cover the 193 participating countries, any treaty is bound to include "loopholes to do a wide range of things" in national regulation, Black said.

But the U.S. cedes the high ground because its "do as we do record is poor," Black said. Intellectual property "is a cutting-edge, wedge issue here." It's easy for other countries to use high-minded social goals to justify regulation when they see the U.S. as "willing to sacrifice freedom for dollars and copyright," he said. **— *Louis Trager***

Hearing June 15

Backpage.com Secures Temporary Restraining Order Against Washington Sex-Ad Law

Under fire from state attorneys general since Craigslist closed its adult services section (WID March 2 p8), Village Voice Media's Backpage.com classifieds site won a minor reprieve when a federal judge issued a temporary restraining order against a Washington state law set to take effect Thursday. SB-

6251 is intended to fight child prostitution enabled by online bulletin boards like Backpage and would make it a felony to knowingly publish advertising for commercial sex involving a minor.

Backpage sued the state earlier this week, claiming the law violates the safe harbors in the Communications Decency Act and the Constitution's commerce clause, and that its definitions are too vague for user-generated content websites to know whether they're violating the law. Village Voice Media also owns *Seattle Weekly*, which runs its online classifieds through Backpage. "We believe human trafficking is an abomination that must be stopped," said Liz McDougall, the company's general counsel, following the order: "But SB 6251 is not the answer."

"Backpage.com has shown a likelihood of success on the merits of its claim ... as well [as] irreparable harm, the balance of equities tipping strongly in its favor, and injury to the public interest, justifying injunctive relief," said the order by U.S. District Judge Ricardo Martinez in Seattle. He blocked Attorney General Rob McKenna, the Republican gubernatorial nominee this election, and county prosecutors from enforcing the law through June 19. Martinez scheduled a hearing on Backpage's motion for preliminary injunction for June 15 and told prosecutors and Backpage to file their replies by June 11 and June 13. McKenna's office and other prosecutors haven't responded to the suit, the judge said.

Criticism of Backpage, based on documented incidents of ads posted for child prostitutes in the Seattle area, has made strange bedfellows across the state, with liberal Seattle Mayor Mike McGinn and rival alt-weekly *The Stranger* joining with conservative McKenna to denounce Village Voice Media. McGinn pulled the city's advertising from *Seattle Weekly* and convinced other mayors to bring pressure on the company to verify the ages of those posted in sex ads online. McKenna has used his position as head of the National Association of Attorneys General to get all but two of his peers to demand the company provide a detailed description of how it weeds out sex ads for minors, in light of *Seattle Weekly*'s required in-person age verification before running sex ads in print.

The Washington state law "will force, by threat of felony prosecution, websites and others to become the government's censors of users' content," the Backpage suit said. Anyone who "causes directly or indirectly" the publication of content that includes an explicit or even "implicit" offer of sexual contact for "something of value," if a minor in fact is depicted, would risk five years in prison and a $10,000 fine per incident, the suit said. The state's claim the law isn't unreasonable, because sites like Backpage would have an "affirmative defense" if they can show they checked the identification of a person to be offered in sex ads, would mean that "every service provider — no matter where headquartered or operated — must review *each and every* piece of third-party content posted on or through its service," the suit said: "These obligations would bring the practice of hosting third-party content to a grinding halt."

"Well-settled federal law" prohibits the Washington law, the suit said, citing Section 230 of the Communications Decency Act (CDA), which blocks interactive computer service providers from being treated as the publisher of third-party content and "expressly preempts" contrary state laws. The First and Fifth amendments prohibit laws that "severely inhibit and impose strict criminal liability on speech" and the commerce clause prevents states from regulatory activity beyond their borders, which "unfortunately" has also happened with a similar law in Tennessee and similar measures under consideration in New Jersey and New York, the suit said. Backpage and its peers could face "a daunting choice: block significant amounts of third-party content, most of which is lawful, or gamble against the risk of felony criminal charges, penalties and imprisonment."

The suit portrays McKenna as duplicitous, citing comments his office made in explaining why he didn't join other attorneys general who were pressuring Craigslist to ditch its adult services section — "it

could cause users to post the same ads elsewhere" on Craigslist and make it harder to police the site. McKenna admitted "shortly after" becoming head of the attorneys general group that they had "little legal standing to forcibly shut down" Backpage and that such sites have "broad immunity" under the CDA. Backpage has "attempted to cooperate" with the attorneys general short of shutting down its adult category, and it already runs ads through "automated filtering and two rounds of manual review of individual postings" to flag suspicious posts, the suit said. It invoked McKenna's gubernatorial campaign as a motivating factor, saying that "on a website promoting his gubernatorial campaign" he called for Congress to amend CDA Section 230 to remove legal roadblocks to taking action against sites like Backpage.

McKenna's office mocked Backpage's lawsuit against the state, disputing the site's claim in a May *Seattle Times* op-ed that it's an "ally in the fight against human trafficking." Backpage wants to "kill a law written to reduce the number of children posted for sale online," McKenna said, calling SB-6251 a "groundbreaking law" (http://xrl.us/bna5yr). McKenna, who has called Backpage "the online marketplace for prostitution," said in August his office had found more than 50 cases of child prostitution on Backpage in 22 states. His office declined to comment otherwise on the suit. — ***Greg Piper***

EAS Goes Online

New EAS Alerts Distributed Online Draw Web Players' Interest

Major websites are interested in getting emergency alert system feeds becoming available over the Internet now that the government and EAS participants are implementing a new format, federal officials and broadcasters said. The Federal Emergency Management Agency's integrated public alert and warning system makes it possible for websites to get real-time access to EAS messages, noted FEMA IPAWS Director Antwane Johnson on an agency webinar Wednesday. Traditional EAS participants in the broadcasting and pay-TV industries are getting ready for the Common Alerting Protocol message format that distributes the alerts online, which the FCC has required be able to be received and passed on starting at month's end, FEMA and FCC officials noted.

"Other private sector entities can monitor the EAS feed as a means of distributing EAS alerts via Internet services, for example Google, AOL, Pandora," Johnson said. "And there are a number of others that are currently in negotiations with us." FEMA's IPAWS open platform for emergency networks is being frequently tested, Johnson and other government officials said. It's meant to be a secondary means of distributing warning messages, Johnson and other FEMA officials said. Spokeswomen for AOL, Google and Pandora had no comment.

Microsoft may be among the other companies interested in getting access to alerts online, since they're becoming available in Internet Protocol format that websites can tap into, said Tennessee Association of Broadcasters President Whit Adamson. IP "gives us something to sell," he said of the "public notices" that, because they're in IP, are "expected to save a lot of money in government." CAP "gives us a lot of reason to talk about our new world, and not just the legacy systems," Adamson said. Tennessee's emergency management agency isn't expected to initially send warnings in CAP, and will remain in EAS, he told us.

There ought to be interest among websites getting access to the IPAWS Internet feeds of other states that do switch to the new format, Adamson told us: But "you can't always depend on that Internet"

getting alerts to EAS participants. The primary entry point stations that get alerts directly from FEMA and whose broadcasts are received and passed on by other stations and pay-TV systems don't always work without flaw, he noted. Adamson cited last year's nationwide test of EAS, the first ever, in which some PEP stations got bad audio in the feed from FEMA and then passed on that glitch to other EAS participants. Satellite feeds that EAS participants can tap into instead generally seem "pretty dependable and pretty good quality and pretty accessible," Adamson said. Another nationwide EAS test hasn't been scheduled, IPAWS Programs Manager Manny Centeno said on the FEMA webinar.

The FCC has found there can be "a single point of failure" in alerts being passed on by respective links in the daisy-chain of stations, said Public Safety Bureau Policy Division Associate Chief Greg Cooke. "Even though on paper this looks fine, you can see this single point of failure goes all the way down the track." States with a "lot of hops using the classic EAS system" can have this problem, Cooke said. "We need to figure out a way of knowing going into the door that we don't have these kinds of single points of failure" beyond the first local primary stations, he said. States that switch from traditional EAS to CAP must tell the bureau of the change, Cooke said. "While we believe CAP is the wave of the future, it is augmenting the systems that you already have in place," he said. "This is just a new layer on the cake." Twenty-four state and local governments are using IPAWS, Johnson said.

CAP doesn't replace "traditional EAS" for "analog reception and the other monitoring sources," and is "a complementary and an additional avenue to deliver the exact same alerts," said IPAWS Deputy Director Wade Witmer. "There will probably be some learning as we implement CAP." FEMA developed the format. All radio and TV stations and subscription-video providers and satellite-radio must be able to get and receive messages in CAP at month's end, although many states and others that send warnings can't yet originate messages in that format, government officials said. Traditional EAS will continue to be available.

The U.S. continues to add PEP stations that get the feeds directly from FEMA and then broadcast them to other EAS participants, Johnson said. There are 63 PEP stations running now, and by September there will be 77 covering 92 percent of the U.S. population, he said. State and local alerts can be sent to IPAWS and then cellphones, as carriers are gearing up to get the alerts, he said. Because the alerts are distributed online, EAS participants must have broadband access, said FEMA officials. They recommended EAS participants have a connection of at least 1 Mbps, with "polling" of the CAP feed every 30 seconds. Most alerts will be about 10 kilobytes in size, "but then there's always the one that has an attachment like an audio file" and those will be larger, a FEMA official said. The agency estimates there will be about 250 alerts sent daily that on average will total 1 megabyte. FEMA has about 150 memorandums of agreement with companies developing alerting capabilities, Johnson said: "That's a real plus for us, with the active engagement and involvement of the private sector" to "craft" and "distribute the warnings" all over the U.S. — ***Jonathan Make***

'Substantial Harm' Feared

FTC Urges Limits on Use of Patents to Exclude IT and Telecom Products

The FTC said International Trade Commission exclusion orders in favor of a standard essential patent (SEP) holder, where infringement is based on implementation of standardized technology, "has the potential to cause substantial harm to U.S. competition, consumers and innovation." It made the statement

in response to an ITC request for comments in Investigation Nos. 337-TA-745 and 337-TA-752. The cases involve products such as iPhones and Xbox 360s.

"These investigations appear to present an issue of first impression for the ITC that has significant implications for the public interest," the FTC said. "Simply put, we are concerned that a patentee can make a RAD [reasonable and nondiscriminatory] commitment as part of the standard-setting process, and then seek an exclusion order for infringement of the RAD-encumbered SEP as a way of securing royalties that may be inconsistent with that RAD commitment."

The FTC said firms in the IT and telecom industries often solve interoperability problems through voluntary consensus standard-setting by standard-setting organizations ("SSOs"). "Interoperability standards can create enormous value for consumers by increasing competition, innovation, product quality and choice," the FTC said. But that agency said incorporating patented technologies into standards also "has the potential to distort competition by enabling SEP owners to negotiate high royalty rates and other favorable terms, after a standard is adopted, that they could not credibly demand beforehand, conduct known as 'patent hold-up.'"

"Hold-up ... can deter innovation by increasing costs and uncertainty for other industry participants [and] can distort investment," the FTC said. It also said the threat of hold-up may reduce the value of standard-setting.

Instead of granting an exclusion order, which limits the ability to import a particular product, the FTC said the ITC could decide Section 337's public interest factors support denial of an exclusion order unless the holder of the RAD-encumbered SEP has made a reasonable royalty offer. Or the ITC could delay the effective date of its Section 337 remedies until the parties mediate in good faith for damages for past infringement or an ongoing royalty for future licensed use, the FTC said.

The FTC comments prompted a posting by Microsoft Deputy General Counsel David Howard on a company blog (http://xrl.us/bna424). He read them in the context of Microsoft's ongoing patent-royalty dispute with Google's Motorola Mobility over the Xbox system. Howard said the FTC statement "adds to the growing chorus of regulators and other government officials around the world who agree that injunctions and exclusion orders based on standard essential patents jeopardize competition and the availability and price of consumer technology."

Industry standards "don't sound like something you should spend a lot of time worrying about," Howard said, but "industry standards are the behind-the-scenes underpinning to wireless connectivity and the Internet, indeed, a foundation on which virtually all modern electronic devices and networks are built." He said standards work because companies and inventors promise to make any patents they hold on the resulting standard available on reasonable and nondiscriminatory licensing terms. "The system depends on these promises, and when companies break them, the system breaks down," Howard said. "Costs go up and popular technology products become less available."

Motorola "decided to break the system by using its standard essential patents to block other companies from selling their products," Howard said. "Google, Motorola's new owner, had the opportunity to reverse Motorola's abusive policies, but has chosen instead to embrace them."

The ITC investigation involves wireless devices, portable music and data processing devices, computers and components. It's based on a complaint filed by Motorola Mobility that alleges violations of

Section 337 of the Tariff Act of 1930 in the import into the U.S. and sale of mobile devices, software and components that infringe patents asserted by Motorola.

The Association for Competitive Technology said the app ecosystem "affects millions of Americans and provides real, tangible benefit to their lives." Given "the economic and public value of our industry, ACT's members are deeply concerned about the impact of an exclusion order in a case where a patent is the subject of a commitment to license on 'Reasonable and Non-Discriminatory' terms as part of a standard," the association's Wednesday filing said. "We believe that granting an exclusion order for 'Standard Essential Patents' is against the public interest."

Microsoft said industry participation in standards-setting is "a risky process" and companies like Motorola that abuse it harm the public interest. Its ITC filing said Motorola promised to participate in the standards-setting on a reasonable and nondiscriminatory basis, and shouldn't be allowed to profit by convincing the ITC to exclude imports of products that allegedly use its patents.

Apple said an "exclusion order is not an appropriate remedy where the complainant is obligated to license its patents to the respondent on fair, reasonable, and non-discriminatory ('FRAND') terms." It said "any exclusion order should exempt replacement parts and units so that consumers who have paid for insurance and warranties can continue to obtain the appropriate repair services."

The Business Software Alliance wants all patentees "free to exercise their intellectual property rights as they see fit," it said. "But if they make the choice to participate in the creation of technology standards and in the process commit to licensing their technologies on fair, reasonable and non-discriminatory ('FRAND') terms, then they should not be allowed to circumvent their original commitment by using the Commission to obtain an exclusion order which could result in extracting unreasonable royalties."

Verizon Wireless said an exclusion order involving smartphones could limit consumer choice and national innovation. Hewlett-Packard said such an order "would thwart competition, stifle innovation, and result in higher prices for consumers — thereby causing precisely the harms that Congress directed Section 337 should not inflict." The Retail Industry Leaders Association said "exploitation of 337 exclusion orders in this manner to obtain artificially high royalties will inevitably result in reduced competition, stymied innovation of standard-compliant products and artificially inflated prices of products for consumers." — ***Michael Feazel***

Capitol Hill

The leaders of the House and Senate Intelligence committees plan to launch a formal investigation to determine who had leaked information about U.S. cybersecurity efforts, they said in a press conference Thursday. The call for a leak investigation came on the heels of several media reports about a classified project called "Olympic Games" which allegedly helped develop and launch cyberweapons against Iranian nuclear facilities. Senate Intelligence Committee Chairman Dianne Feinstein, D-Calif., refused to specify exactly the nature of the leaks nor confirm that the U.S. had helped develop and launch a cyberweapon against Iran. Feinstein said the Senate will work to include changes to the Intelligence Authorization Bill "to codify processes in retarding leaking" in the next month or so. She would not say whether any changes to House and Senate cybersecurity bills would be needed. Committee Vice Chairman Saxby Chambliss, R-Ga., said he was "extremely upset" by the "cascading leaks" that put lives in danger and

"infringes" on the intelligence community's ability to do its job. House Intelligence Committee Ranking Member Dutch Ruppersberger, D-Md., said he did not think the leaks were politically motivated, as has been alleged by some lawmakers. He urged members of Congress and the White House to work with investigators to find out who was responsible for the leaks, and determine how to prevent them in the future. "We need to change the culture of leaks generally ... only those that need to know are going to know." Chambliss said he wanted to get to the bottom of the issue to find out who was responsible for the leaks. "Where the chips fall, they fall." House Intelligence Committee Chairman Mike Rogers, R-Mich., said the leaks are "incredibly damaging" and he hopes to put legislation together quickly to stem the "serious and growing problem."

———

Bipartisan national security experts favor regulation of critical infrastructure in cybersecurity legislation, they said in a letter made public by Senate Commerce Committee Chairman Jay Rockefeller, D-W.Va., a sponsor of the Cybersecurity Act (S-2105), which has such a regulatory bent. The letter to Senate Majority Leader Harry Reid, D-Nev., and Minority Leader Mitch McConnell, R-Ky., said Congress should take swift action on such legislation. "Infrastructure that controls our electricity, water and sewer, nuclear plants, communications backbone, energy pipelines and financial networks must be required to meet appropriate cyber security standards," said former Homeland Security Secretary Michael Chertoff, former Director of National Intelligence Mike McConnell, former Deputy U.S. Secretary of Defense Paul Wolfowitz, former CIA Director Michael Hayden, and others (http://xrl.us/bna72t): "Where market forces and existing regulations have failed to drive appropriate security, we believe that our government must do what it can to ensure the protection of our critical infrastructure."

Agencies

Media trade associations urged the FCC to grant a temporary exemption or waiver to its IP-video closed captioning rules sought by the Digital Media Association (DiMA). The MPAA, NCTA and NAB jointly filed comments supporting DiMA's request (http://xrl.us/bna6ki). "The current unrealistic deadline for implementing the complete set of Enhance Features ... does not serve the best interests of consumers," they said. Such "enhanced features" include technical controls that let consumers manipulate the appearance of captions, they said. "While hardware manufacturers have until January 1, 2014 to implement the Enhanced Features, video programming distributors only have until the first software update after September 30, 2012 to begin making those features available in applications or plug-ins they provide to consumers," they said. "This much more aggressive timeframe for VPDs is unrealistic, and there is no reason to expect the task assigned to VPDs is any easier to achieve than that required of device makers."

Privacy

"Smart device owners are becoming increasingly concerned about others accessing private content on their mobile devices," NQ Mobile reported Thursday based on the results of a survey it had done. "Nearly a quarter of those surveyed feel someone close to them may have already secretly accessed the content on their smart phones, including employers, friends, significant others and even their own children." NQ's Mobile Vault is a new Android application that allows device users to store with encryption and password protection their contacts, SMS messages, call logs, photos and videos. The survey was taken online in March of 1,000 adult regular users of smartphones and tablets. The sample wasn't random, so no probability of error is meaningful, the company said.

Security

Tumblr is an increasingly popular playground for cybercriminals, a report about online threats in May found. Attacks on Tumblr users included "two spam campaigns centered around a fake 'Tumblr Dating Game,' fake advertising spam asking for personally identifiable information in exchange for ad revenue generated by the victim's tumblelog, and a phishing site posing as the Tumblr login page," GFI Software researchers reported Thursday. One of them, Christopher Boyd, said, "More and more, cybercriminals are exploiting the familiarity of terms and images in order to distract the victim from the dangers that are present as they sign away their personal information and click on links that lead to nothing but trouble."

———

Verizon said it translated its 2012 data-breach report (WID March 23 p11) into six more languages — French, German, Italian, Japanese, Portuguese and Spanish (http://xrl.us/bna4yf). "The more people we can touch through our computer forensics work, the better prepared we all are to fight cybercrime," said Wade Baker, Verizon director of risk intelligence. It's the first time the company has published the annual report in a language other than English, a spokeswoman told us.

Internet People

Univision Communications promotes **David Beck** to vice president-general manager of new social media team ... WPP's 24/7 Media promotes to senior vice president: **Rob Schneider** for corporate strategy and development and **Ellen Kamor-Graham** for account management and tech support ... TechAmerica Foundation panel on "big data" adds as academic co-chairs: **Michael Rappa**, North Carolina State University, and **Leo Irakliotis**, Western Governors University.

Washington Internet Daily

(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, Washington Telecom Newswire, Telecom A.M., Television & Cable Factbook, Cable & Station Coverage Atlas and other special publications.

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

Copyright © 2012 by Warren Communications News, Inc.
Reproduction in any form, without written permission, is prohibited.

Phone: 202-872-9200 Fax: 202-318-8984
www.warren-news.com
E-mail: info@warren-news.com

EDITORIAL & BUSINESS HEADQUARTERS
2115 Ward Court, N.W., Washington, DC 20037

Albert Warren
Editor & Publisher 1961-2006

Paul Warren . . . . . .Chairman and Publisher
Daniel Warren . . . . . .President and Editor
Michael Feazel . . . . . Executive Editor
Paul Gluckman . . . . . Senior Editor
Mark Seavy . . . . . Senior Editor
Jeff Berman . . . . . .Senior Editor
Howard Buskirk . . . . . Senior Editor
Dinesh Kumar . . . . . .Senior Editor
Jonathan Make . . . . . Senior Editor
Rebecca Day. . . . . Senior Editor
Tim Warren . . . . . Assistant Editor
Kamala Lane . . . . . Assistant Editor
Bryce Baschuk . . . . . Assistant Editor
Matthew Schwartz . . . . . Assistant Editor
Brian Feito. . . . . Assistant Editor

Louis Trager. . . . . Consulting News Editor
Josh Wein. .. . . . . West Coast Correspondent
Greg Piper . . . . . Seattle Correspondent
Barry Fox . . . . . Contributing 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

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

Sales

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

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.