



WARREN'S Washington Internet Daily

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

FRIDAY, MAY 13, 2011

VOL. 12, NO. 93

Today's News

IP-CASE WIRETAPS should be authorized by Congress because of sophistication of infringers, says head of DOJ criminal division. (P. 1)

OBAMA'S CYBERSECURITY PLAN advocates more DHS authority during cybersecurity events, FISMA revision. (P. 2)

EU 'CHINESE WALL' to fight child abuse online under discussion by European governments. (P. 3)

COICA SUCCESSOR puts enforcement ability in hands of DOJ, IPR holders. Protect IP Act allows 'blacklist' of sites, groups say. (P. 4)

CAPITOL HILL: Barton, Markey are no-shows at their own mobile privacy briefing ... Bills offered to block 'unfair' taxes on digital goods ... Lawmakers ask SEC to push companies for more transparency on cybersecurity breaches. (P. 6)

AGENCIES: FTC reaches \$3 million settlement with Playdom for COPPA violations ... Conflict of interest concerns raised about Baker staying at FCC until she goes to Comcast ... NIST want comments on cloud-computing guide. (P. 8)

DOJ's Criminal Division Chief Stumps for Wiretap Power in IP Investigations

SAN FRANCISCO — The Department of Justice needs wiretapping authority concerning intellectual property infringements to keep up its vigorous enforcement, the head of the department's criminal division said Thursday. Justice has broadened its use of tapping in general under the Obama administration, and the expansion into copyright and trademark cases is needed so the department can use the technique "as an effective tool in the future," Assistant Attorney General Lanny Breuer said in a keynote to the International Anti-Counterfeiting Coalition conference.

Overall, "this administration has made intellectual property enforcement a higher priority than any other administration in recent memory," Breuer said. "We are absolutely committed to fighting back." Copyright and other intellectual-property offenses aren't included in the crimes that federal law allows wiretapping orders on, he told us after his speech. So Justice asked Congress in March to expand its authority, Breuer said. The change is needed because IP infringements are often the product of "sophisticated operations," he said. The chances that the change will be enacted are "very strong," Breuer said.

New technologies are exploited by individuals and organized criminal enterprises to create high-quality knockoffs and perfect digital copies for global distribution," Breuer said. He added, "Websites that offer pirated or even prerelease copies of movies, music, software or games often operate overseas. The reason is simple: Not every country takes IP enforcement as seriously as we do or has the expertise to prosecute IP cases effectively." That's why the department stresses international training and cooperation, he said.

Breuer asked those listening to "continue educating the public about the scourge of IP crime." There's "a misperception that IP

crimes are victimless or that victims of IP crimes don't really suffer," because the violations seem "more abstract to most people than stealing a car," he said. That view "has a counterproductive effect on our efforts," and in reality infringement kills jobs and companies, Breuer said. He also asked companies to work to detect infringements of their rights as they happen and to report violations right away. "We cannot police the entire world economy," and DOJ can't respond as "efficiently and aggressively" if it learns of an infringement "long after the fact," he said. — *Louis Trager*

Lacks 'Kill Switch'

Lawmakers Give Qualified Praise to White House Cybersecurity Plan

The White House released its cybersecurity plan Thursday, and urged lawmakers to fortify the nation's cybersecurity, critical infrastructure and federal networks. Notably absent from the proposal was any "kill switch" authority for the president to shut down Internet traffic during a cyberattack. Lawmakers applauded the White House move, but some said it was long overdue and made clear they wanted changes or provisions added from their own legislation. The plan was more than two years in development.

The Department of Homeland Security should lead the nation's cybersecurity response, the report said, and lawmakers should expand DHS authority to address and modify the U.S. response to cybersecurity threats. The administration also suggested that DHS provide assistance to organizations victimized by cyberattacks and advocated better overall information sharing efforts between the public and private sectors.

The proposal seeks legislative changes in order to improve federal cybersecurity, it said. The plan specifically asks Congress to revise the Federal Information Security Management Act (FISMA), enhance intrusion prevention systems, increase federal cybersecurity recruitment and migrate to secure, cloud-based federal data storage. Any and all federal cybersecurity efforts must implement strong privacy protections and a cybersecurity framework that respects civil liberties, the White House said.

The proposal advocates greater corporate and federal transparency after data breaches and enhanced penalties for computer criminals. Critical infrastructure operators, which include the electricity grid, the financial sector and U.S. transportation networks, should employ third-party commercial auditors to identify and prioritize the U.S. critical infrastructure vulnerabilities, the report said.

The White House proposal got a cautious nod from Senate Commerce Committee Chairman Jay Rockefeller, D-W.Va., and Sen. Olympia Snowe, R-Maine, sponsors of a cybersecurity bill that failed to move last year. Rockefeller and several other Senate committee chairmen sponsored a "broad placeholder" bill at the direction of Senate Majority Leader Harry Reid, D-Nev. (WID Jan 27 p4). Rockefeller called the White House proposal a "strong plan" that incorporates many elements of his bill with Snowe, such as close collaboration with business, and adds consumer protections for data breaches. Snowe said the "administration's delay in providing critical input to the legislative process is regrettable," but otherwise echoed Rockefeller's comments. She said she told White House cyber coordinator Howard Schmidt Thursday morning that the administration must "come before Congress very soon to brief us on the reasoning behind its proposals." Reid said separately that relevant Senate committees would "integrate their work" with the White House proposal in "coming weeks" and build on protections in legislation passed last Congress.

The White House proposal is a "welcome and necessary addition" to the Senate Homeland Security Committee's work, said Chairman Joe Lieberman, I-Conn., Ranking Member Susan Collins, R-Maine, and

Federal Financial Management Subcommittee Chairman Tom Carper, D-Del., in a joint statement. The Lieberman-Collins cybersecurity bill drew antipathy for a "kill switch" provision that was read as giving the President the authority to cut off Internet traffic in some circumstances, a provision later removed (WID March 8 p6). "The Senate and the White House are on the same track" with regard to protecting cybernetworks and critical infrastructure through public-private cooperation, "risk-based assessments" and the DHS lead on the matter, they said.

Congressional Cybersecurity Caucus co-founder Rep. Jim Langevin, D-R.I., also faulted the White House for having "moved slowly toward implementing" the recommendations from the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency, which Langevin co-chaired. The White House proposal, while echoing some provisions Langevin has championed, "still leaves some areas of concern," he said: It neglects to designate a cyber director to handle interagency coordination or lead a National Office for Cyberspace, or even give DHS authority over cybersecurity policy. "Congress must revisit this issue," Langevin said. He said he also wants the administration to weigh in "more heavily" on the U.S. military posture in cyberspace, a subject Langevin took up at Wednesday's markup of the National Defense Authorization Act.

TechAmerica called the White House proposal "a clear step forward" for the public-private cyber partnership. It should promote an "outcome-based, layered security approach" adopted voluntarily by business and avoid a "one-size-fits-all, mandated approach to cybersecurity," the group said. The proposal also needs to draw a "bright line between critical and non-critical infrastructure" and lay out the "implications" for that designation, and provide liability protections for companies operating at the government's behest, TechAmerica said.

The Information Technology Industry Council gave the proposal a backhanded compliment. The White House showed "much-needed leadership" on cybersecurity by offering the proposal, though "any first draft won't be perfect," said CEO Dean Garfield. The group suggested that the proposal doesn't yet promote "extensive collaboration" between business and government. "The cybersecurity debate of 2011 is much different" than in years past, "and it's clear that policymakers need to carefully assess how we effectively adapt to emerging threats, technologies and business models," Garfield said. Software and Information Industry Association President Ken Wasch thanked the administration for promoting collaboration, providing resources for R&D, embracing cloud computing, and blocking states from requiring "localized IT infrastructures" under the proposal. — *Bryce Baschuk, Greg Piper*

No EC Blacklist Plans

Proposal to Make ISPs Virtual Border Guards Said Serious But Likely Not Feasible

EU governments are considering a "virtual Schengen border" in cyberspace to block illegal child abuse content, documents posted Thursday by European Digital Rights showed. The idea has been kicking around for some time, but the Council made available a PowerPoint presentation, "towards a single secure European cyberspace," that was shown to ministers in February and obtained pursuant to a freedom of information request by Article 19: the Global Campaign for Free Expression. The fact that the proposal was on the Council's Feb. 17 agenda shows it's serious, but it's unclear whether the idea has legs, Article 19 Senior Legal Counsel David Banisar told us. The European Commission has "no plans to introduce specific blocking lists," or "black lists," a Home Affairs spokeswoman said.

The real Schengen regime is a unified visa system that allows visitors to participating countries to cross borders with few or no checks, its website says. The council's law enforcement working group said Feb. 17 that it would propose concrete measures for a cyberborder and for making ISPs "virtual access points" to stop illicit materials on the basis of an EU-wide blacklist, council conclusions said. The presentation "does not reflect the official opinion of the Council, the General Secretariat of the Council or the [EU] Presidency," the letter to Article 19 said.

The PowerPoint gives examples of sites inside and outside the EU that published child abuse content, and discusses possible solutions to the problem. Blocking has worked locally in some countries, such as Italy, in cases of child pornography, the presentation said. Other countries, such as Germany, have laws requiring ISPs to block such content, it said. In others, non-governmental organizations use hotlines for reporting illegal content to appropriate authorities, it said. But the working group said it prefers a joint solution that involves law enforcement, NGOs and the private sector.

ISPs "are the virtual 'border crossing points' at the EU's computer technology and Internet 'borders,'" the presentation said. Actions can only be effective if all European ISPs use the Internet in a coordinated manner and at the same time, it said. Police agencies, courts and NGOs can maintain the blacklists, it said. But blocking pedophile content is only the first step, it said. If EU members agree, the cooperative effort can be extended to other kinds of crimes such as counterfeit medicines, it said.

The presentation makes clear that the intent is to use child abuse as a hook to gain political support for the process, EDRI said on its website. It also shows that the content to be blocked would be "sufficiently trivial that it is possible that it would not be illegal in the country where the material is hosted," it said. The proposal, moreover, doesn't even mention prosecution, even when the content is hosted in the EU, it said.

The reality is that the EU can't impose a Schengen-like border on the Internet, Banisar said. Governments can limit what ISPs are allowed to disseminate, but the Internet is so vast that no amount of blacklists will prevent the content from spreading, he said. Whitelists of approved websites would likely be outlawed by the European Convention on Human Rights, he said.

This all goes to the ongoing debate on the role of Internet intermediaries, Banisar said. There's strong pressure to get ISPs to do more, whether in policing their networks for intellectual property violations or combating anti-terrorism and child pornography activities, he said.

U.S. virtual exports won't fare well if ISPs are forced to build walls, EDRI Advocacy Coordinator Joe McNamee said. If, as the U.S. Combating Online Infringement and Counterfeits Act also proposes, virtual borders are created all over the world, with new bottlenecks and "gatekeepers," those virtual products won't as successful as they would be in an open market, he said. — *Dugie Standeford*

Digital 'Theft' Measure

New Legislation Allows AG, Copyright Holders To Pursue 'Rogue' Site Operators

New legislation from Sens. Patrick Leahy, D-Vt., Orrin Hatch, R-Utah, and Chuck Grassley, R-Iowa, focuses on protecting intellectual property by cracking down on "rogue" websites dedicated to the sale of infringing or counterfeit goods. The Protect IP bill follows the Leahy-led bill, the Combating

Online Infringement and Counterfeits Act (COICA), which won support from the Senate Judiciary Committee last year. The new measure, S-968, will help protect consumers, jobs and “the investment American companies make in developing brands and creating content,” said Leahy, committee chairman, in a written statement. The bill also would give law enforcement and copyright holders tools to bring actions against rogue sites, the statement said. A leaked draft of the bill emerged earlier this week, but the committee said it wasn't finished (WID May 12 p6).

The bill contains updated provisions stemming from the COICA bill, the committee said. It defines a “site dedicated to infringing activities” as one that “has no significant use other than engaging in, enabling or facilitating the reproduction, distribution or public performance of copyrighted works,” the bill said. It authorizes the Attorney General and rightsholders to bring actions against online infringers operating a site or domain, “but with remedies limited to eliminating the financial viability of the site, not blocking access,” the committee said. After the Attorney General takes action, financial transaction providers, ISPs and information location tools shall take reasonable and feasible measures to disable or suspend service to the site, the bill said.

Domain name registries, registrars, payment processors, ad networks and other parties are shielded from damages “resulting from their voluntary action against an Internet site dedicated to infringing activities, where that site also endangers the public health, by offering controlled or non-controlled prescription medication,” the committee said.

The Protect IP Act has drawn support from some entertainment groups, intellectual property rights advocates and organized unions, like American Federation of TV and Radio Artists and the Directors Guild of America. However, other groups like Demand Progress and Public Knowledge expressed significant concerns. Under the bill, foreign sites would be hindered from taking advantage of U.S. IPR, some entertainment groups said in a press release. These sites “would no longer be allowed to exploit U.S. registrars, registries, ISPs ... and ad placement services to sustain their illicit online businesses,” said MPAA, Independent Film & Television Alliance and others.

Viacom, the Software & Information Industry Association and the Copyright Alliance applauded the bill's attempt to give law enforcement more tools to go after websites. “For consumers, the legislation will help reduce consequences like identity theft, viruses, or receipt of defective, unregulated and dangerous products due to unwittingly engaging with criminals online,” Copyright Alliance Executive Director Sandra Aistars said.

Establishing the rules that will make it easier for legitimate participants in the marketplace to access consumers while blocking infringing sites “makes enormous sense,” said David Hirschmann, president of Chamber of Commerce’s Global IP Center, during a conference with representatives from the Information Technology and Innovation Foundation, the Copyright Alliance and other groups. “It attacks the income stream which is the heart of the devastation that the music industry has suffered,” said Rick Carnes, Songwriters Guild of America president.

The new measure is worse than COICA, said Demand Progress. The ability of the Attorney General and copyright holders to take action against sites is “sure to result in an explosion of dubious and confused orders,” the group said. “The PROTECT IP Act is like a virtual '1984' where ISPs and browsers would be forced to send any mention of blacklisted sites down the memory hole,” said Aaron Swartz, executive director. “The bill as written can still allow actions against sites that aren't infringing on copyright if the site is seen to ‘enable or facilitate’ infringement — a definition that is far too broad,” Public Knowl-

edge said. The bill amounts to "an acquiescence to the content lobby's idea that everyone whose systems touch their content has a price to pay — if not in direct dollars, then in deputized vigilance on their behalf," Deputy Legal Director Sherwin Siy said. — *Kamala Lane*

Capitol Hill

The co-chairs of the House privacy caucus were kept from showing up to their own briefing on location-based services Thursday. Reps. Edward Markey, D-Mass., and Joe Barton, R-Texas, scheduled the briefing but were unable to attend because they had to vote on a separate issue. Spokesmen for Markey and Barton said the lawmakers are working on a children's privacy bill, but would not release a time line for the bill's introduction. Separately, Markey and Barton scrutinized Facebook for alleged privacy issues stemming from a Wednesday *Wall Street Journal* article about the company's third-party use policies. The article said some advertisers and other unauthorized third parties have been able to access and use Facebook user accounts for years. Markey and Barton sent a letter to Facebook CEO Mark Zuckerberg asking for details about the data leakage, the company's investigation into the matter and its plans to inform users about the problem. "This issue is one that cannot be ignored and our concerns about Facebook's privacy policies are continuously increasing," they said. Groups invited to participate in Thursday's privacy briefing made opening statements before the lawmakers' aides ended the briefing. Andrea Williams, CTIA vice president-law, said a carrier-centric approach to privacy guidelines is "no longer appropriate or applicable," and location-based service providers must act to reduce the risk of surreptitious and unauthorized tracking. Location-based service providers should give users ultimate control over their data by obtaining prior consent and disclosing to consumers how they use their data in plain, easy to understand language, she said. Facilitating both the growth of location-based services and protecting user privacy are paramount to the mobile privacy debate, said Marc Rotenberg, executive director of the Electronic Privacy Information Center. Rotenberg advocated an "expeditious establishment of comprehensive, technology neutral privacy protections" and urged lawmakers to think about the privacy debate from the consumer perspective. Morgan Reed, executive director at the Association for Competitive Technology, said Congress is unfairly targeting small application development companies for the privacy violations committed by large service providers like Google and Apple. Application developers don't generally collect a "whole lot of data," said Reed; instead they collect a small amount of data and pass it on to third parties. Reed asked that Congress not forget about developers in any upcoming legislation and give small businesses more leverage to deal with any upcoming changes to Google and Apple's privacy policies. — **BB**

Another data protection bill surfaced in the House. Rep. Cliff Stearns, R-Fla., reintroduced the Data Accountability and Trust Act (DATA), which he originally offered in the 109th Congress. Rep. Bobby Rush, D-Ill., last week introduced HR-1707, a duplicate of Rush's DATA bill from the 111th Congress. And House Commerce Manufacturing Subcommittee Chairwoman Mary Bono Mack, R-Calif., has said she's working on legislation based on Rush's DATA Act but updated to reflect recent events like the Sony data breach. Rep. Jim Matheson, D-Utah, cosponsored the Stearns bill, HR-1841. "This bill represents a bipartisan approach to address growing security concerns, and would protect consumers from security breaches," Stearns said. "As more and more commerce is done electronically, there remains a need for strong and specific security practices for businesses that keep personal information." HR-1841 requires the FTC to require owners of personal and other electronic data to write security policies and procedures. It also would require that consumers are notified of security breaches if there's a risk of identity theft. Stearns said he looked forward to working with Bono Mack, who didn't co-sponsor his bill. Bono Mack "is working diligently on her own bi-partisan bill which we will move through our subcommittee in the not-too-distant future," a Bono Mack spokesman said.

Digital goods could not be taxed at higher rates than tangible counterparts under House and Senate bills offered Thursday. The Digital Goods and Services Tax Fairness Act (HR-1860) by House Judiciary Committee Chairman Lamar Smith, R-Texas, and Administrative Law Subcommittee Ranking Member Steve Cohen, D-Tenn., would prevent "unfair" taxes on, say, MP3 downloads relative to CDs, Smith's office said. "While books are still sold in stores across the country, readers can now download hundreds of digital books, newspapers and magazines" online or from mobile devices, Smith said. Sens. Ron Wyden, D-Ore., and John Thune, R-S.D., introduced companion legislation in the Senate. The Administrative Law Subcommittee plans a hearing on the bill later this month, Smith's office said. A similar bill from Sens. Ron Wyden, D-Ore., and John Thune, R-S.D., seeks to protect mobile smartphone apps, cloud computing and other digital goods and services from additional taxes. The bill, S-971, establishes a framework for fairness across many tax jurisdictions, Wyden's office said. State and local governments would be prohibited from applying taxes to products that don't apply to similar tangible goods, it said. Legislation also states that "when the legitimate taxes are imposed on a digital product, it can only be imposed on the final customer or end user." There are limitations placed on retail, sourcing, treatment of digital codes, bundled goods and taxpayer, the bill said. Taxes can only be imposed by state and local jurisdictions "whose territorial limits encompass the customer's tax address," the bill said. Digital services include the provision of remote access to or use of a digital good, but does not include telecom services, Internet access service or audio or video programming service, the bill said. The House and Senate measures were applauded by USTelecom, CTIA, Download Fairness Coalition and other groups. They offer a "smart solution to unnecessarily complex state and local tax policies that could be unfair to consumers and stifle economic growth," Verizon said. A tangle of varying and discriminatory taxes "will confuse consumers and place an unfair financial burden on those who choose to go online to make certain purchases," said USTelecom President Walter McCormick. Once passed, the legislation "would provide tax administrators and consumers a better understanding of how music, books and other downloadable products should be taxed," CTIA President Steve Largent said.

The House Judiciary Committee approved legislation extending three provisions of the Patriot Act expiring May 27. In a markup Thursday, the committee voted on partisan lines 22-13 to approve HR-1800. The bill would extend by six years provisions on roving wiretaps and Section 215 orders to obtain "any tangible thing," and permanently extend a "lone wolf" provision. The committee shot down a plethora of amendments offered by Democrats. One by Rep. Hank Johnson, D-Ga., would have required roving wiretap targets to be described with greater detail in order to avoid surveillance of innocents. But Rep. Tom Marino, R-Pa., said that would make it easier for terrorists to conceal their identities. Marino also called it "a solution in search of a problem" because he said there's been no evidence of problems with the current roving wiretap provision. Johnson also offered an amendment to prevent collection of location information from cellphones and other electronic devices belonging to U.S. citizens not suspected of terrorist activities. But Rep. Trey Gowdy, R-S.C., said the issue was unrelated to the legislation at hand and should be discussed at "another time and place." The Senate Judiciary Committee in March approved a bill (S-193) to extend the expiring provisions by three years. — **AB**

Lawmakers asked the SEC to push companies for more transparency about cybersecurity breaches, in a letter released Thursday. Senate Commerce Committee Chairman Jay Rockefeller, D-W.Va., and four other Democrats signed the letter, including Sens. Sheldon Whitehouse, R-I., Richard Blumenthal, Conn., Robert Menendez, N.J., and Mark Warner, Va. They specifically asked the commission to issue guidance to companies about their disclosure requirements concerning security risks and "material network breaches." Current corporate disclosures of material data breaches are "inconsistent and unreliable," the senators wrote, despite federal laws that require disclosure of any material network breach. "We are concerned that the lack of quality and public information in these matters enables an inefficient marketplace that devalues security and impairs investor decision-making," the letter said. The senators also

asked the SEC to report on how credit rating agencies and securities analysts incorporate corporate security risks into their assessments. Recent high profile cyberattacks on Sony and Epsilon have increased congressional focus on corporate data security.

Agencies

The FTC reached a \$3 million settlement with Playdom, an online multiplayer gaming company, stemming from charges that it violated the rules of the Children's Online Privacy Protection Act (COPPA), the FTC said Thursday. The FTC charged that the company, which operates 20 "virtual world" websites, "illegally collected and disclosed personal information from hundreds of children under age 13 without their parent's prior consent." The \$3 million settlement was the largest civil penalty for a violation of the COPPA rule, the FTC said.

FCC Commissioner Meredith Baker faces potential conflicts of interest, even if she is recusing herself from any proceeding involving her future employer Comcast (WID May 12 p1), several critics of agency procedures said in interviews Thursday. Baker surprised many by saying Wednesday she'd leave the FCC. She's restricted in what she can do until she departs June 3 to lobby for Comcast's NBCUniversal in Washington, and other restrictions will take effect after she starts work for the cable and broadcast programmer. Baker's office and representatives of FCC Chairman Julius Genachowski aren't saying what, if any, proceedings she has sat out of since she began talks for the job last month. Recusal from the several pending proceedings directly relating to Comcast may not be enough for Baker, said President Craig Aaron of Free Press, a critic of both the agency and the cable operator. WealthTV CEO Robert Herring said Baker's departure worries him because the independent cable programmer has an order on its complaint against Comcast circulating on the eighth floor. The resignation further highlights what some call Washington's revolving door between regulators and the companies they oversee, said Craig Holman, a lobbyist for Public Citizen. Free Press on Thursday asked its members to write their members of Congress to "stop the revolving door" and "demand Congress investigate Baker's conflict of interest." "There are rules that govern situations like this," Genachowski said at a news conference following Thursday's FCC meeting, which Baker skipped. "I expect that Commissioner Baker has and will comply with all of those rules. She has been in touch with the general counsel and the chief ethics officer" of the commission, he added. On questions of the "revolving door," Genachowski said "there are rules in place, there are strict rules. Compliance is very important and I think they'll continue to be." Baker was contacted by Comcast about working there in the second half of April, FCC General Counsel Austin Schlick told reporters Thursday. He declined to disclose the exact date: "I'll let Commissioner Baker give the date if she likes." After Baker "was contacted by Comcast, the commissioner in accordance with our recommended practice for senior officials" contacted the General Counsel's office, Schlick said: "We worked closely with her." Baker must recuse herself from any commission business involving Comcast from the time she began job discussions, Schlick said: She must also avoid the "appearance" of a conflict of interest. He declined to say if Baker recused herself from the items voted on Thursday, or if she is sitting out any other matters at the FCC. May 2, an order dismissing WealthTV's program carriage complaint against Comcast circulated, as did an order and rulemaking on program carriage rules that would affect Comcast, agency officials have said. Other examples of pending proceedings at the FCC affecting Comcast in a significant enough way that Baker should sit them out completely are on AllVid rules for all pay-TV companies to connect to consumer electronics equipment and media ownership rules, said Aaron and Corie Wright, a policy counsel at Free Press. "We're looking into any potential conflicts of interest," Wright said. "It seems like Commissioner Baker has some explaining to do" and "we hope she'll be in attendance at tomorrow's House subcommittee hearing to answer some of these questions," she added. Baker won't be testifying. Warren Communications News, publisher of *Washington Internet Daily*, filed a Freedom of Information Act request with the FCC on Thursday to be given a list of all proceedings Baker was recused

from and the date when she first told commission officials she was considering employment elsewhere. Herring filed his own FOIA request, too, he said. "Did Commissioner Baker or her staff participate in discussions of WealthTV's complaints, including but not limited to File No. CSR-7907-P, after she initially engaged in job solicitation discussions with Comcast?" was among the questions he submitted Thursday to the regulator. "Has Commissioner Baker or her staff been given access to the circulated item(s) post Commissioner Baker's initial job solicitation with Comcast?" Herring worries that even though Baker may have recused herself from WealthTV's program carriage complaint against Comcast, her staff may have sat in on internal meetings at the commission where the case was discussed, he said in an interview. Under Section 2641.201 of the U.S. Criminal Code, Baker is banned permanently from representing Comcast on any "particular matter in which [she] participated personally and substantially." Other parts of the code call for two-year restrictions on lobbying on matters "for which the employee had official responsibility," a one-year restriction "on any former senior employee's representations to former agency concerning any matter, regardless of prior involvement," and a two-year restriction "on any former very senior employee's representations to former agency or certain officials concerning any matter, regardless of prior involvement." — *JM, BM*

A News Corp. unit argued against AllVid rules, which the FCC may soon propose so all consumer electronics can access pay-TV programming without CableCARDs. "Marketplace developments are superseding the need for government action when it comes to the retail availability of devices consumers use to access video" at home, Fox Group said. It cited a subscription-video company carrying Fox programming that told the company it will soon make programming including VOD available to "widely-marketed" CE devices such as game consoles. A Fox executive spoke with FCC Chief of Staff Eddie Lazarus, the company said in a filing Wednesday in docket 10-91. TiVo meanwhile asked the commission to "carefully monitor the progress and implementation" of pay-TV providers' work with CE manufacturers for the equipment to access distributors' programming. "We hope that other pay-TV providers follow Comcast's lead," TiVo said in a filing posted Tuesday to docket 97-80, citing a deal between the two companies. TiVo was an initial member of a coalition that formed recently to seek AllVid rules, along with Google, Sony and others.

The National Institute of Standards and Technology said it wants comments on its *Cloud Computing Synopsis and Recommendations* guide, Special Publication 800-146, which explains cloud computing in "plain terms and provides practical information" for information technology decision makers considering a cloud move. Federal CIO Vivek Kundra tasked NIST with leading federal efforts on standards for data portability, cloud interoperability and security. "Since cloud computing spans a spectrum of underlying technologies and configuration possibilities, each organization's requirements call for different cloud technologies and configurations" — guidance found in the new publication, said project leader Lee Badger. The guide is at <http://xrl.us/bki46b>. Comments are due June 13 at 800-146comments@nist.gov.

Courts

Defunct P2P software maker Lime Wire and the RIAA were in settlement talks Monday and Wednesday following testimony at a damages trial last week, according to the docket in the five-year-old *Arista v. Lime Wire* copyright infringement case. A previous attempt at settlement at a May 3 conference overseen by U.S. District Judge Kimba Wood was "unsuccessful," the docket said. A spokeswoman for the RIAA told us there was no update for Thursday. Lime Wire was ordered to shutter its LimeWire P2P client after losing the case last fall, which included a finding of personal liability for founder Mark Gorton (WID Oct 28 p1). CNET reported Thursday that lawyers were still negotiating a possible settlement, citing multiple sources. The last major P2P settlement was with Kazaa, which paid \$115 million in 2006 to settle infringement claims with the record and film industries. — *GP*

Industry Notes

The mobile app has yet to deliver revenue for mobile video programming suppliers, SNL Kagan said in a white paper about domestic mobile video trends. Verizon's decision to drop VCast Video as part of its wireless data subscription package hurt mobile video revenue and "since apps were not producing revenue and Verizon was pulling away, 2010 was the slowest year of revenue growth on record for U.S. mobile video," it said. But now about a third of all wireless customers have a smartphone, which makes viewing video easier, and tablet PCs are on the rise, it said. TV broadcasters hoping to participate in the mobile video market "still face the challenge of offering compelling mobile service that excites an audience now accustomed to time shifting," it said. And mobile video ad sales have been a "slow starter," and are expected to account for less than 10 percent of all mobile video revenue in 2011, it said.

The PlayStation Network shutdown wasn't impacting Ubisoft significantly, Ubisoft CEO Yves Guillemot said in an earnings call. It was "affecting the games that we launched and it's affecting some games that we wanted to launch" but had "to be delayed," he said. But he said "the impact is still small because our revenue on" the platform is "not huge," so "the cost will be minimal." Ubisoft makes "significantly" more revenue from Xbox Live Arcade than PSN, so it was "better for us that it's not the XBLA that is in trouble today," he said. But he said it was "important that" Sony "restore the system quickly because lots of our products are multiplayer games" that use PSN. — **JB**

Internet People

Local.com promotes **Michael Sawtell** to chief operating officer, replacing **Bruce Crair**, leaving for other opportunities ... Cloud.com hires **Ken Kim**, ex-Symantec, as vice president and general manager of Asia-Pacific ... Demand Media promotes **Taryn Naidu** to executive vice president for registrar services and general manager of eNom domain name wholesaler, replacing **Michael Blend**, who will now work on special projects.

 <p style="text-align: center;">(ISSN 1530-0501) PUBLISHED BY WARREN COMMUNICATIONS NEWS, INC.</p> <p>Michael Feazel Managing Editor Dugie Standeford European Correspondent Scott Billquist Geneva Correspondent</p> <p>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.</p> <p style="text-align: center;">Send news materials to: newsroom@warren-news.com</p> <p style="text-align: center;">Copyright © 2011 by Warren Communications News, Inc. Reproduction in any form, without written permission, is prohibited.</p> <p>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</p>	<p style="text-align: center;">WASHINGTON HEADQUARTERS Albert Warren <i>Editor & Publisher 1961-2006</i></p> <p>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</p> <hr style="width: 20%; margin: 10px auto;"/> <p>Louis Trager Consulting News Editor Josh Wein West Coast Correspondent Greg Piper Seattle Correspondent</p> <p style="text-align: center;">Television & Cable Factbook</p> <p>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</p>	<p style="text-align: center;">Business</p> <p>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</p> <p style="text-align: center;">Sales</p> <p>William R. Benton Sales Director Agnes Mannarelli National Accounts Manager Jim Sharp Account Manager Brooke Mowry Account Manager Norlie Lin Account Manager</p> <p style="text-align: center;">NEW YORK BUREAU 276 Fifth Ave., Suite 1002, N.Y., N.Y. 10001 Phone: 212-686-5410 Fax: 212-889-5097</p> <p>Paul Gluckman Bureau Chief Mark Seavy Senior Editor Jeff Berman Senior Editor Rebecca Day Senior Editor Razia Mahadeo Editorial Asst. Barry Fox Contributing Editor</p>
<p>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.</p>		