

2 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 25, 2008 Monday

LENGTH: 286 words

HEADLINE: GOP Convention-Goers to Have Workshops on User-Generated Content

BODY:

Republican conventiongoers will get a "crash course" in social media and mobile Internet platforms Democratic foes have used to "run circles" around them, a convention organizer told us. Debi Jones, a former Netscape, Palm and Microsoft executive, will produce GOP Unconventional, a social media workshop track and Web site focused on the Republican convention in Minneapolis.

Lifelong Democrat Jones wanted to take emerging technologies and new media to both conventions, she said. But the Democratic National Committee credentialed only a few bloggers, keeping them mostly offsite, she said.

The Republicans have given media passes to more than 200 bloggers, according to Jones and a party spokesman. Both said the party was impressed with a similar educational project that Jones ran this year at CTIA and invited her to produce an educational track and online channel emphasizing live video.

The workshops will train and equip delegates to "create their own media," Jones said. Two pre-convention classes will explain how to use Qik live streaming via Nokia and Samsung hardware to produce "behind the scenes" video, and how to upload photos to the Web and use microblogging platforms like Twitter.

Content created by Jones' "students" will be collected and organized on GOPUnconventional.com. Jones will produce a nightly special highlighting "best of" moments ignored by broadcasters. The workshops, software and infrastructure are sponsored by Qik, Mogulus, Cradlepoint and Microsoft.

Several prominent Republican politicians and their aides will participate, Jones said. She wouldn't identify them. She hopes the experience inspire lawmakers to use the technology in their daily work, she said. - Andrew Feinberg

3 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 22, 2008 Friday
Correction Appended

LENGTH: 741 words

HEADLINE: Critics Question NCMEC Role in Policing Web for Child Porn

BODY:

Internet service providers' voluntary agreements with state attorneys general to cooperate more closely on child porn highlight the role of the National Center for Missing and Exploited Children. The federally-funded nonprofit center seems to be taking on duties usually handled by police agencies and its activities raised serious due-process questions, critics told us.

Federal law requires the center to create a "blacklist" of URLs tagged as "known child pornography sites" -- in the words of NCMEC President Ernie Allen, the "worst of the worst." A memorandum of understanding with NCMEC requires many major ISPs to enforce the list.

Web sites aren't told they're on the blacklist and can't appeal their listings beyond having NCMEC "verify" that a site no longer hosts illegal content, Allen said. The center checks the sites on its own "every day" to see if material is taken down, he said.

The list is off-limits to outsiders. When we asked to see part of it, Allen said the center refuses to release the list, including to the media. Access to the list could lead someone to view an outlaw image, a federal crime, he said. NCMEC provides the list only "law enforcement and to Electronic Service Providers that enter into an MOU with us... We are working very hard to ensure that the list is current and that URLs that no longer contain illegal content are removed from the list immediately," through "active, daily communication" with ISP signers. News media could report wrongly that a site is on the list after it has been removed, Allen said.

And telling site owners they're "blacklisted" could jeopardize enforcement, Allen said. ISPs are required by law to take down offending material, he said, but not to notify the content owner.

Who Gets the Power?

NCMEC's expanding role raises significant questions, said the Progress & Freedom Foundation's Adam Thierer. He's a member of the Internet Safety Technical Task Force organized by Harvard's Berkman Center to work on Internet safety tools. Several ISPs and Web companies take part, along with NCMEC. The task force, born of MySpace's tangles with states over child safety, reports quarterly to attorneys general. It was to make formal recommendations by year-end, but they have been put off to the first quarter of 2009 (WID July 25 p4).

The task force hasn't focused on child porn, Thierer said. Instead, it has concentrated on age verification methods and ways to keep youngsters from accessing content. He expressed concern that stressing the center's "blacklist" means "turning a blind eye" to those creating the porn, a process scarcely affected by pressuring ISPs.

A private body, NCMEC doesn't come under the Freedom of Information Act, and isn't accountable for its methods in creating its "blacklist," Thierer said. Without independent review, Thierer said, he's concerned by the center's ability to create a list that the law requires ISPs to enforce. "Is that a power for a private institution?" he said.

The center works with liaison officers from the FBI, Secret Service, Immigration and Customs Enforcement and other agencies, Allen said. But by law NCMEC alone makes the list. Allen and Thierer both said there is no "due process" for someone whose site is on the list to have it removed. Allen said he doesn't see this as a problem, since the center's procedures ensure that sites stripped of illegal content come off the list, he told us. But NCMEC wouldn't say how often or how thoroughly the list's accuracy is verified.

NCMEC checks blacklisted sites "every day" and procedures in place are sufficient, Allen said. He repeatedly reminded us that listed sites carry the "worst of the worst" content, voicing confidence that if such content disappears from a URL, it comes off the list. NCMEC can maintain an up-to-date list, he said, repeatedly discounting the chances of a URL landing on the list by mistake.

NCMEC isn't operating as a law enforcement agency, Allen said. The center's liaison agencies exercise their individual powers, he added.

Mark Esser, chairman of the California ISP Association, endorsed the center's activities but said he sees "a lack of legal due process for anyone who is wrongfully added to the list." The center's goals are admirable, but the NCMEC system is fatally flawed, Thierer agreed. Thierer expressed deep concern over the precedent set by the NCMEC process: "This is the beginning of the making of a body of secret law." - Andrew Feinberg

CORRECTION-DATE: August 26, 2008

CORRECTION:

Federal law does not require the National Center for Missing and Exploited Children to maintain a list of claimed child porn Web sites (WID Aug 22 p1). The center maintains the list for ISPs that have signed memoranda of understanding with it.

4 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 22, 2008 Friday
Correction Appended

LENGTH: 741 words

HEADLINE: Critics Question NCMEC Role in Policing Web for Child Porn

BODY:

Internet service providers' voluntary agreements with state attorneys general to cooperate more closely on child porn highlight the role of the National Center for Missing and Exploited Children. The federally-funded nonprofit center seems to be taking on duties usually handled by police agencies and its activities raised serious due-process questions, critics told us.

Federal law requires the center to create a "blacklist" of URLs tagged as "known child pornography sites" -- in the words of NCMEC President Ernie Allen, the "worst of the worst." A memorandum of understanding with NCMEC requires many major ISPs to enforce the list.

Web sites aren't told they're on the blacklist and can't appeal their listings beyond having NCMEC "verify" that a site no longer hosts illegal content, Allen said. The center checks the sites on its own "every day" to see if material is taken down, he said.

The list is off-limits to outsiders. When we asked to see part of it, Allen said the center refuses to release the list, including to the media. Access to the list could lead someone to view an outlaw image, a federal crime, he said. NCMEC provides the list only "law enforcement and to Electronic Service Providers that enter into an MOU with us... We are working very hard to ensure that the list is current and that URLs that no longer contain illegal content are removed from the list immediately," through "active, daily communication" with ISP signers. News media could report wrongly that a site is on the list after it has been removed, Allen said.

And telling site owners they're "blacklisted" could jeopardize enforcement, Allen said. ISPs are required by law to take down offending material, he said, but not to notify the content owner.

Who Gets the Power?

NCMEC's expanding role raises significant questions, said the Progress & Freedom Foundation's Adam Thierer. He's a member of the Internet Safety Technical Task Force organized by Harvard's Berkman Center to work on Internet safety tools. Several ISPs and Web companies take part, along with NCMEC. The task force, born of MySpace's tangles with states over child safety, reports quarterly to attorneys general. It was to make formal recommendations by year-end, but they have been put off to the first quarter of 2009 (WID July 25 p4).

The task force hasn't focused on child porn, Thierer said. Instead, it has concentrated on age verification methods and ways to keep youngsters from accessing content. He expressed concern that stressing the center's "blacklist" means "turning a blind eye" to those creating the porn, a process scarcely affected by pressuring ISPs.

A private body, NCMEC doesn't come under the Freedom of Information Act, and isn't accountable for its methods in creating its "blacklist," Thierer said. Without independent review, Thierer said, he's concerned by the center's ability to create a list that the law requires ISPs to enforce. "Is that a power for a private institution?" he said.

The center works with liaison officers from the FBI, Secret Service, Immigration and Customs Enforcement and other agencies, Allen said. But by law NCMEC alone makes the list. Allen and Thierer both said there is no "due process" for someone whose site is on the list to have it removed. Allen said he doesn't see this as a problem, since the center's procedures ensure that sites stripped of illegal content come off the list, he told us. But NCMEC wouldn't say how often or how thoroughly the list's accuracy is verified.

NCMEC checks blacklisted sites "every day" and procedures in place are sufficient, Allen said. He repeatedly reminded us that listed sites carry the "worst of the worst" content, voicing confidence that if such content disappears from a URL, it comes off the list. NCMEC can maintain an up-to-date list, he said, repeatedly discounting the chances of a URL landing on the list by mistake.

NCMEC isn't operating as a law enforcement agency, Allen said. The center's liaison agencies exercise their individual powers, he added.

Mark Esser, chairman of the California ISP Association, endorsed the center's activities but said he sees "a lack of legal due process for anyone who is wrongfully added to the list." The center's goals are admirable, but the NCMEC system is fatally flawed, Thierer agreed. Thierer expressed deep concern over the precedent set by the NCMEC process: "This is the beginning of the making of a body of secret law." - Andrew Feinberg

CORRECTION-DATE: August 26, 2008

CORRECTION:

Federal law does not require the National Center for Missing and Exploited Children to maintain a list of claimed child porn Web sites (WID Aug 22 p1). The center maintains the list for ISPs that have signed memoranda of understanding with it.

5 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 21, 2008 Thursday

LENGTH: 390 words**HEADLINE:** New Media Front and Center in Convention Coverage**BODY:**

Traditional coverage of the Democratic and Republican conventions will be supplemented by legions of bloggers and "citizen journalists," brought together through online "Convention Hubs" run by C-SPAN and announced Aug. 12, officials said. The sites, which go live later this week, will provide a forum for bloggers to comment on the goings-on from outside the convention and will serve a central repository for bloggers credentialed by the parties and allowed floor access, said officials at C-SPAN and New Media Strategies, the company coordinating the hubs.

"C-SPAN has always tried to target the largest possible audience" said producer Ben O'Connell, the network's coverage coordinator in Denver for the Democratic convention. C-SPAN consciously decided to use technology that was "new to us" to widen its reach, he told us.

The highest profile part of C-SPAN coverage will be embeddable video, a feature that O'Connell called a C-SPAN first. Not only will bloggers be able to clip and embed any network's video streams for their blogs, but casual viewers can search, capture and e-mail clips, he said.

At both conventions, bloggers credentialed by the parties to cover the floor will have their own space on the site, with C-SPAN providing aggregation of both "national" bloggers, such as Daily Kos on the left and RedState on the right, and bloggers "embedded" with state delegations.

New and emerging technologies are probably the most exciting thing that C-SPAN is doing, O'Connell said. Not only will C-SPAN be aggregating Twitter "tweets" from the conventions using "hashtags" #DNC08 and #RNC08, but the channel also will have two roving cameras using Qik streaming video. And C-SPAN has created a group at which bloggers and citizen journalists can post their Qik streams to C-SPAN's convention hubs, allowing anyone with a suitable camera to provide coverage. C-SPAN will Skype and related technology to air interviews with personages at distant locations, he said.

C-SPAN won't restrict itself to "preapproved" bloggers credentialed by the parties, O'Connell said. Anyone following and writing about the conventions can e-mail material that C-SPAN will run if it's found worthwhile, he said. The C-SPAN Convention Hubs will be available this week at www.c-span.org/politics/DNC08 and www.c-span.org/politics/RNC08 - Andrew Feinberg

7 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 19, 2008 Tuesday

LENGTH: 161 words

HEADLINE: Consumers Getting News from Varied Sources

BODY:

Consumers no longer make "either-or" choices in seeking news, Pew Research Center said. Nearly a quarter of consumers, including a well-educated, middle-aged group called "integrators," get news from conventional sources and the Internet, said the study, released Sunday.

TV remains the main news source for about two-thirds of integrators, but the Internet is cited by more than a third of integrators as their primary daytime news outlet, since they use the Internet to monitor events during working hours. And the overall proportion of Americans who get news online rose to 37 percent, up six points from 2006. Daily use of online news sources rose about a third, from 18 percent in 2006 to 25 percent in 2008.

Multimedia distribution contributes to the Internet news rise, the report said. Just under a third of Internet news consumers watch online video news, and 19 percent listen to it online in both streaming and podcast form, the survey said. - Andrew Feinberg

9 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 15, 2008 Friday

LENGTH: 278 words

HEADLINE: 'Free Software' Licenses Can Protect Copyrights

BODY:

Software developers using so-called free or open-source licenses can enforce them with lawsuits, ruled a three-judge panel of the U.S. Court of Appeals for the Federal Circuit. Ruling Wednesday, the court said the open-source "artistic license," which requires derivative works to credit original author, does not create an "intentionally broad" license, as a district judge had ruled.

Violating the license doesn't breach a contract, it breaks copyright law, the court said. Saying open-source licensing "has become a widely used method of creative collaboration that serves to advance the arts and sciences in a manner and at a pace that few could have imagined just a few decades ago," the court cited entities like MIT.

Open-source licenses cover software that underlies much of the modern Internet, including the Apache Web Server, Mozilla's Firefox Web browser and the Linux operating system itself, the opinion said. It pointed to an amicus brief by Creative Commons estimating that more than 100,000 creative works are under licenses it wrote.

Such licenses have great value, the court said: "Improvement to a product can come rapidly and free of charge from an expert not even known to the copyright holder. The Eleventh Circuit has recognized the economic motives inherent in public licenses, even where profit is not immediate."

Of particular importance is the absence of dispute as to who owned the copyright to the code in question, the court said. Instead, the dispute before the court was whether copyright law was enforceable when a copyright holder had given up some rights. The court said it was, remanding the case to the district Court. - Andrew Feinberg

12 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 11, 2008 Monday

LENGTH: 229 words

HEADLINE: Facebook, under Cyberattack, Says Users Should Exercise Caution

BODY:

An apparent vulnerability in Facebook's "wall" feature allowed the rapid spread of a worm-style virus, said Max Kelly, the company's head of security. The company blocked links to a video-sharing site hosting malware that clicking on the links installed, he said.

The bug was first reported by analyst Michael Arrington late Thursday, prompting a flurry of alerts and the release of a "patch" by Facebook early Friday. Kelly wrote a response late Thursday on the company blog calling the attack a run-of-the-mill "phishing" scam being spread by "spam" messages and wall posts and saying Facebook was working on a fix to block the malicious site. Kelly said the problem affected only 0.002 percent of Facebook users.

The problem appeared to be confined to Windows machines, Arrington later wrote. He criticized Facebook's "blocking" solution as a "black list approach" meaning a "never ending battle."

The hole was a known issue, Social Times' Nick O'Neil said in a blog post Friday. But this time it affected enough people to come to the attention of the user community, prompting action from the company. O'Neil later wrote that the fight against spammers and hackers would only intensify as the company grows, and actions like blocking links to malicious sites would be one part of "their ongoing fight." We couldn't reach Facebook representatives for comment. -- Andrew Feinberg

14 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 08, 2008 Friday

LENGTH: 484 words**HEADLINE:** IRS Scrutinizing Charity Web Site Links**BODY:**

The Internal Revenue Service is watching the Internet, especially tax-exempt groups Web content, during this year's campaign, according to documents on its Web site. A July 28 memo to agents monitoring 501(c)(3) organizations indicates that the IRS is bearing down on use of links this political season.

The IRS has wanted to check charities' compliance since it began work on political activities in the 2004 campaign, Lois Lerner, then agency director of exempt organizations, said in an April letter. This year's work aims to exert a "meaningful enforcement presence," the letter said. That includes monitoring exempt organizations' links to other Web sites, the July memo said.

Web site operators always have been responsible for monitoring linked sites' content, said tax lawyer John Hoover. The rules for 501(c)(3) entities on the Web are not unlike those for other activities, he said. There's no "strict liability" for Web site operators, he said. But the IRS memo indicates that the agency is "not shying away" from studying charities' online activities, he said. Examples of what is and is not permitted in terms of linking appear in a June 2007 IRS decision that continues to guide enforcement.

A "safe harbor" letting a charity link to the "home page" of a related 501(c)(4) organization indicates only that for now the IRS has no interest in the issue, Hoover said. But so-called deep linking to specific pages on a related entity's site is prohibited, he said.

"Context is king" in analyzing whether a link constitutes political activity, said election-law attorney Jeff Hunter. IRS rules are clear on whether a link is allowed, based on context within the originating site and the site being linked to, he said. A link to a factual newspaper article with a link to an editorial page is allowed, but a direct link to the editorial itself is not, Hunter said. He added that there's a risk of confusion arising from Federal Election Commission rules on online activity. The FEC worries about whether money changes hands in exchange for speech, and the IRS looks at the content of speech, Hunter said.

Social networks and new media platforms probably won't require new IRS rules, Hoover said. But without specific guidance they remain a "grey area," he said. If an exempt organization embeds a YouTube video it created on its own Web site, and after it's played YouTube offers a political ad that an algorithm alone determines is "related," there probably is no problem, Hoover said. "You would have to point to control" over how the "related" content is displayed to find a violation, he said.

The same principle probably applies to social networking sites, Hoover said. Should the linked profile of a non-profit's online "friend" endorse or oppose a candidate, the organization probably needn't monitor the linked content unless such oversight is "reasonably" feasible, he said. - Andrew Feinberg

15 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 05, 2008 Tuesday

LENGTH: 420 words**HEADLINE:** Microblogging Shines Light on GOP Sit-In, May Signal New Online Momentum for Party**BODY:**

House Republicans who stayed behind in Washington after a vote to adjourn found an unlikely medium to spread word about their activities. Announcement of their "sit-in" was made Friday by Rep. John Culberson, R-Texas, using his Twitter microblogging account from the House floor (WID Aug 1 P6). He and Rep. Pete Hoekstra, R-Mich, "tweeted" the goings-on in the chamber as Republicans refused to leave the floor for several hours, culminating in a press conference late Friday. Around the same time, Eric Dojom, a Chicago-based social media consultant put up a website, dontgo.us, named after the "hashtag" used to track conversation about the events. The site has since received several thousand visitors and rising, he said.

Twitter enables messages to spread like "ripples from a pebble in water," said Julie Barko Germany, director of George Washington University's Institute for Politics and Democracy on the Internet. While anecdotal evidence may suggest that Twitter has enabled the House GOP message to get past the "inside the beltway" crowd, she cautioned that this technology is new enough that there are no quantitative studies on its use. But she said it allows politicians to "reach out to people who will spread the message for them" in a place more visible than the more partisan blogosphere, where Democrats have had much more success.

The phenomenon may be explained by the percentage of bloggers and journalists on the service, said Colin Delaney, editor of ePolitics.com. Delaney suggested there was no partisan divide in use of the service despite the active promotion of politicians like Culberson.

Twitter's success among the GOP is a "pleasant surprise" to Patrick Ruffini, an e-campaign strategist for Bush-Cheney '04. "When there are no microphones, no cameras... how else could the message get out?" he asked. Michael Turk, who was Ruffini's boss at Bush-Cheney and now works in grassroots advocacy at NCTA, compared the situation to a 2005 incident when then-House Judiciary chairman James Sensenbrenner, R-Wis., closed a hearing in face of Democratic protests. Turk said this is no surprise to him: "A lot of us ... have said that once [the GOP] was in the minority, they would begin to adapt these tools in a new way."

The difference between 1995 and now is that new media allows more communication, Turk said. He was in Chicago when the "revolt" started, but thanks to Twitter, he told us he was able to observe and participate in the discussion "like he was there, on the floor." - Andrew Feinberg

18 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
SATELLITE WEEK

August 04, 2008 Monday

LENGTH: 553 words**HEADLINE:** Reforming Space Agency is Texas Lawmaker's Passion**BODY:**

Unmanned exploration and scientific research have been neglected at NASA because of political considerations, Rep. John Culberson, R-Texas, told us in an interview last week. Funding for the space program should not be a choice between manned and unmanned, he said. "I'm a big fan of both parts of the space program," he said. "But if the agency were driven by the scientists, engineers, and astronauts that do the work rather than political considerations, I think you'd see the entire spectrum of work NASA does funded adequately." The four-term congressman's district is home to many Johnson Space Center workers.

Under Culberson's plan, NASA would have the freedom to create its own budget based on recommendations by "an independent panel of scientists and engineers and astronauts," he said. The panel would be able to tell appropriators "how much money NASA actually needs and what it should be spent on" year to year, he said.

Culberson is trying to enlist the support of House Science Committee chairman Bart Gordon, D-Tenn., in a plan to "completely restructure" the agency. Culberson is adamant that it's time to rethink NASA, despite drawing fire from the agency and a Democratic opponent after he said it "wastes a vast amount of money" during a July town hall meeting.

Culberson knows that real reform won't come easily. "This is a sweeping, broad change that will take some time," he said. He told us that he has had extremely positive feedback from both sides of the aisle among members equally frustrated by problems with NASA's budget and bureaucracy. Responding to critics who question his commitment to space, Culberson was blunt: "I love the space program - if I didn't care, I wouldn't try to fix the problems."

Restructuring NASA has been on Culberson's mind for the past few months, he said. But wasn't ready to talk publicly about the matter until the town hall incident. "I made a blanket statement that doesn't apply to the whole agency," he said. But reforming the agency's 50 year old bureaucracy would "help NASA spend the money we do give them much more wisely," he said. "The space program should be driven by science, not politics."

"No one has been a bigger advocate or supporter of the space program than I have," Culberson told us. Despite a history of fiscal conservatism, he regularly proposes and votes to increase money for NASA as a member of the House Commerce, Justice and Science Appropriations Subcommittee. But the agency has problems ranging from an outdated bureaucracy to inefficient personnel policies, such as its inability to hire and fire based on performance, he said.

NASA should be independent of the executive branch, said Culberson. "We need to get them out completely free of the Office of the President...so they are not under the thumb of the White House." The space agency should be able to make "independent, objective budget recommendations to the Congress without regard to political pressures," he said. Vexed that the White House hasn't submitted adequate budgets for the space agency to excel, he had particularly harsh words for "bean counters" he says shortchange many important space program projects. "I don't frankly count the

number from OMB it's not giving us a number based on what's good for science," he said. "Let NASA run NASA." -
Andrew Feinberg

19 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

August 04, 2008 Monday

LENGTH: 1814 words**HEADLINE:** Comcast Discriminated against P2P Traffic, FCC Votes 3-2**BODY:**

By 3-2, FCC commissioners found that Comcast discriminated against P2P applications by interfering with them but not other broadband traffic. FCC Chairman Kevin Martin's Republican colleagues dissented, as expected (WID Aug 1 p1). Martin and Commissioner Jonathan Adelstein criticized Comcast for not being candid with consumers and the FCC about its network management. They and Commissioner Michael Copps called the practices discriminatory and in violation of 2005 FCC net neutrality principles. Commissioner Robert McDowell criticized consideration of the order because major changes were shared with other commissioners but not him the evening of the vote. He disagreed with acting against Comcast after it had agreed not to discriminate and for enforcing principles that aren't rules.

Comcast wasn't fined but could face further enforcement action if it violates the order. The action gives the company 30 days after the document's release to reveal "the details of its discriminatory network management practices," tell the FCC how it will stop them and describe to its broadband subscribers and the commission its revised practices, a commission news release said. Comcast must stop treating P2P traffic differently from other Web applications by year-end under the order. The company has said it will. "All we are doing is requiring them to follow through on the commitment," so "hopefully" the FCC won't have to further act against the company, General Counsel Matthew Berry told reporters. The order has "teeth," he said.

The FCC will be "vigilant" in checking Comcast's diligence in obeying the order, due to be released "very soon," said Wireline Bureau Chief Dana Shaffer. "We call upon the public to monitor Comcast vigilantly," Berry said. If the operator doesn't comply, Shaffer said, "the order makes clear that they will be subject to perhaps injunctive relief and/or further enforcement action."

Comcast violated sections 201, 230, 256, 257, 601 and 706 of the 1996 Telecom Act, Berry said. The cable operator got notice of the threat of FCC action on Web-blocking complaints in a 2006 order approving the \$17 billion takeover of Adelphia by Comcast and Time Warner Cable, Shaffer said. Since Comcast didn't seek reconsideration of the Adelphia order or challenge it otherwise, "it is somewhat disingenuous of Comcast to come back and now dispute the commission's authority," Shaffer said.

Friday's order against Comcast "raises significant due process concerns and a variety of substantive legal questions," a company spokeswoman said. "We are considering all our legal options and are disappointed that the commission rejected our attempts to settle this issue without further delays." Comcast's network management was "reasonable, wholly consistent with industry practices" and didn't block access to Web sites or online applications, she said. NCTA President Kyle McSlarrow said the agency is "second-guessing reasonable network management techniques" and has "no notice or guidelines in place."

Comcast didn't say whether it will appeal. Free Press General Counsel Marvin Ammori said he won't be surprised if

it does. "They tend to appeal most of the decisions at the FCC that don't go their way," he told reporters. Gigi Sohn, president of Public Knowledge, which also complained about Comcast's practices, said the FCC vote was the most significant advancement of the public interest in communications technology in at least 20 years.

The FCC found that Comcast's behavior departed from standard industry practice and the company was "selectively targeting and interfering with practices of peer to peer applications," Shaffer said. The company "compounded the harm" by not going public on its actions, she added, citing a Comcast spokesman's comments to news media that it wasn't blocking access to any application. "Comcast has a substantial anticompetitive motive" to interfere with P2P because those applications let people watch video on the Internet that they could otherwise view on TV, she said.

No broadband provider defended Comcast's actions, Martin said. Comcast was "hiding" what it did "by making consumers think the problem is their own" and "lying about it to the public," he added. Comcast's deep-packet inspection is akin to the post office's "opening your mail, deciding they didn't want to bother delivering it, and hiding that fact by sending it back to you stamped 'address unknown -- return to sender,'" Martin said. Opponents of Comcast's practices have said the company sent "false reset messages" that cut off ongoing communication between network users. Martin said Comcast claimed it was managing congestion caused by a few users sapping capacity with bandwidth-intensive uses, but "the evidence told a different story." It blocked use of BitTorrent and other applications when customers used "very little bandwidth simply because they were using a disfavored application," Martin said.

Comcast gave an "inaccurate response" to early questions about its behavior, Adelstein said. The FCC order is a "narrow" finding, stands on "firm legal ground" and "sets out an important marker" that other ISPs' practices will be subject to "heightened review," he added. It shows that the FCC will take a "case-by-case approach" on network management, he said. The FCC has authority to act and legislation isn't needed, Martin said. Copps said the "landmark" decision doesn't prevent ISPs from "reasonably managing their networks" but keeps the Internet "open." Before the FCC investigation, begun in January by the Enforcement Bureau, decisions about the Internet were "being made in a black box," Copps said.

The order isn't a "monumental decision," Commissioner Deborah Tate said, adding that the complaint dealt with the activities of 5 percent of Internet users. "It seems as if there has been a communication gap between Comcast and its customers" over network management, and all "ISPs must do better." But Comcast's posting usage policies on its Web site showed that the company was responsive.

Technical disputes are best settled "through collaboration and negotiation," and the FCC lacks authority to intervene, McDowell said. The final version of the order changed about half of the earlier draft, he said. In an interview, he said communications among commissioners' offices leading up to the order departed from FCC precedent because not all aides for FCC members were in the loop. "There were significant, substantive changes and the majority did not air those changes on the traditional e-mail chain among offices the way majorities did" in other instances, he said. But Martin told reporters that the final draft was similar to his July 11 public description of the item, and an FCC spokeswoman said commission procedure was followed.

Lawsuits Could Rope in Congress

The commission action shows no law is needed, telecom companies said. "Redoubled industry efforts" on setting practices and explaining them to consumers can avert problems, said Verizon Executive Vice President Tom Tauke. AT&T Senior Executive Vice President Jim Cicconi said the FCC decision not to fine Comcast showed there was no evidence of "anticompetitive intent."

But the decision could lend momentum to legislation, especially if Comcast goes to court, others said. Lawsuits challenging FCC on its network principles could spur Congress to step in, said a Stifel Nicolaus note. If courts find the FCC had no clear rules, a future FCC might adopt rules that cable and telcos "would find far more troubling," it said.

The decision got Hill scrutiny, even as Congress shut down for its summer break. "I do believe legislation is still

needed to clarify that the FCC has the authority" to enforce its rules, Rep. Chip Pickering, R-Miss., told us. But case-by-case enforcement remains the best tack, said Pickering, co-sponsor of a bill (HR-5353) with Telecom Subcommittee Chairman Ed Markey, D-Mass., to give the FCC enforcement power.

The decision "underscores" the need to ensure consumers are protected from network management interference, Markey said. He vowed a push on his bill and pledged to continue monitoring industry practices. The House Commerce Committee will keep exercising "vigorous oversight to ensure that the FCC fully enforces its Internet principles," a committee spokesman said.

Some Republicans said the FCC overreacted. "There has been no market failure to justify the heavy-hand of so-called net neutrality, and I do not believe the Commission has the authority to enforce principles as if they were adopted rules," said Sen. Sam Brownback, R-Kan. He called the Comcast decision a "giant step backward" from Bush administration deregulatory policies.

'Broad Conception' of FCC Power

The vote drew mixed reactions among Internet players. "I think this is a win for the American people and a good first test of the FCC's net neutrality principles," Craigslist founder Craig Newmark told us. The order "sends an important signal that consumers must have open and unfettered access to all of the Internet's resources," said Richard Whitt, senior policy counsel to Google.

David Sohn, senior policy counsel to the Center for Democracy & Technology, said he fears that the final order "probably" will reflect a "broad conception" of FCC power. "We have doubts whether the FCC's current statutory authority really gives them a sound legal basis to do formal enforcement in this area," he said. The FCC order is "an important first step," said Bennett Kelley, founder of the Internet Law Center. He said he was surprised that the first significant government action on network neutrality came from the FCC.

Child safety advocates and content owners are pleased with the order's provisions on "unlawful" content. "We are grateful that the commission reiterated its concern for blocking unlawful content such as child pornography," Carolyn Atwell-Davis, director of legislative affairs for the National Center for Missing and Exploited Children, told us. -- Jonathan Make, Andrew Feinberg, Anne Veigle

* * * * *

The Electronic Frontier Foundation is hoping to scare other ISPs out of using network management by releasing a "testing tool" for connections. "Switzerland" has been available to "technically sophisticated Internet users" as open-source, command-line software that spots packets forged or modified between clients and gives users copies of modified packets, EFF said. But the group plans to "make it easier to use over time," and is soliciting help from developers. Switzerland will spot meddling by products and services from traffic-shaping provider Sandvine, antipiracy filter Audible Magic, advertising system Fair Eagle "and various censorship systems," among others, EFF said. "The sad truth is that the FCC is ill-equipped to detect ISPs interfering with your Internet connection," said Fred von Lohmann, senior intellectual property attorney.

21 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

August 01, 2008 Friday

LENGTH: 661 words**HEADLINE:** OMB Official 'Didn't Want to Embarrass' Underperforming Agencies on IT**BODY:**

The Office of Management and Budget ignored its duty to report yearly to Congress on "major acquisitions" so it would not embarrass federal agencies over budget and behind schedule on IT projects, OMB Administrator for Electronic Government and Information Technology Karen Evans said at a Thursday Senate Government Information Subcommittee hearing chaired by Rep. Tom Carper, D-Del. A major theme was the common practice of "rebaselining" -- jargon for revising timelines and budgets when a project misses the old ones.

Panel chairman Carper pilloried OMB for reporting to Congress only three times since enactment of the 1994 Federal Acquisition Streamlining Act. That law requires annual OMB reports on federal IT projects and spending. A fourth report arrived late Wednesday. Perhaps excessive "rebaselining" explained OMB's spotty record, Carper said. "Someone, somewhere - in my view - is not fulfilling their responsibility to ensure that taxpayer dollars are spent only on those investments that are well thought out and truly necessary," Carper said.

OMB hesitated to release data for fear of embarrassing agencies, Evans said. Her agency has been "struggling" with the extent of what it should release, she added. "How much shame and embarrassment do you bring upon an agency?" she asked. "We're supposed to be helping them."

OMB wants to get results, not to drive compliance, Evans said. If agency personnel expect to be "graded," she said, "people will do just enough in order to get... the grade." Since it's not an auditor, OMB doesn't track how often agencies "rebaseline," Evans said. Carper asked why her office couldn't list overdue IT projects "to allow us to provide proper oversight."

The Bush administration has not wanted to highlight delays caused by budget shortfalls, said David Powner, GAO director of IT management issues. He, too, said OMB was reluctant to embarrass agencies, but said OMB's own data are flawed because the watchdog didn't factor in repeated rebaselining.

Unwillingness to expose weak data is "consistent with this administration's management agenda," Powner said of OMB's concealment of shortfalls and failure to document rebaselining. But chronicling the extent of rebaselining would "drive it underground," Evans said, saying once she addressed rebaselining at the agency level she would have no problem giving Congress data.

OMB has not held agency CIOs accountable for their rebaselining habits, Powner said. Many agencies have recast timelines and budgets without any review by management, he said. OMB has no guidelines for rebaselining, but could write a "framework document," Evans said.

Congress should go after agencies whose IT budgets and project are out of control, Powner said. Oversight could focus on solutions, but more data are needed to characterize the extent of the problem, he said. -- Andrew Feinberg * * *

* * A bill introduced Thursday by Sen. Carper aims to prevent runaway IT projects by requiring federal agency CIOs to develop IT management plans, submit annual reports to Congress on projects and warn the Hill of delays and cost overruns, triggering a process to "pull the plug" on out-of-control projects. The Information Technology Investment Oversight Enforcement and Waste Protection Act of 2008 hadn't been assigned a bill number at our deadline. The measure would require agency CIOs to gather internal quarterly reports on IT projects and notify agency heads, who would tell Congress if a project has a "significant deviation" from projected schedule and costs. Further delays or overruns could cause a "gross deviation," triggering a review of the project that could lead to ending it. The bill would create an expert IT Strike Force to provide requested help for agencies' IT projects. Carper compared the proposed body to specialized teams used by the Navy to retrain underperforming flight crews. The bill is co-sponsored by Sens. Susan Collins, R-Me., and Joseph Lieberman, I-Conn.

24 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 31, 2008 Thursday

LENGTH: 534 words**HEADLINE:** Competition to Google Grows**BODY:**

Successful competitors and new entrants continue to increase the market for search, in the face of fears of a rising Google monopoly expressed in congressional hearings last month (WID July 15 p1). Google, acknowledged as the industry leader, faces challenges from competitors new and old.

Baidu is the undisputed king of China's search market with 64.4 percent of revenue in the second quarter, IRG's weekly stock report said Tuesday. Google's Chinese revenue fell 0.7 percent during the quarter, IRG said. The value of the Chinese search market is up 87 percent from a year ago and should continue to rise as the Beijing Olympic Games increases demand, it said.

Baidu's results back up a June report by comScore Media Metrics, which gave Google a lead in the Asia-Pacific region, but not in all countries. ComScore Executive Vice President Jack Flanagan said country-specific search engines "play a significant role in the region."

Meanwhile, after three years of "stealth mode" development and hype in Silicon Valley circles, Cuil launched its site late Sunday. The new search engine was developed by CEO Tom Costello and Anna Patterson, vice president of engineering, who built pioneering search systems at IBM and Google.

Cuil uses "semantic search" technology to analyze relationships between a user's search term and the information surrounding it on a page, in addition to a conventional ranking systems based on links, said the company Web site. The company said this method takes search a step further by allowing users to "search for ideas." Cuil also takes a poke at Google's practice of collecting and storing user data. A summary of the company's 500-word privacy policy reads: "When you search with Cuil, we do not collect any personally identifiable information, period. We have no idea who sends queries... Your search history is your business, not ours."

Other emerging technologies, are gaining momentum, said a spokesman for comScore. "Human powered search engine" Mahalo has surprised the researchers with rapid growth. It was off comScore's radar with less than 100,000 viewers a month in August 2007, but made a tremendous leap to 1.4 million in June, Flanagan said.

The market still is wide open and has room for innovation, Mahalo CEO Jason Calacanis said in an interview. He acknowledged the power of semantic systems, but said the computing power needed for them is "orders of magnitude" greater than what is available today.

Mahalo uses employees and a wiki-style system for users to create pages offering the most popular links for a particular keyword, as well as background information and news, said Calacanis. When humans filter results for the top one-third of popular keywords from the machine search for clarity and relevance, Mahalo and others like it can connect people with the information they want "better than anybody" else, he said.

There's no reason to fear a search monopoly, Calacanis said. "There are a hundred companies that are pursuing search in a major way. I don't think it is an anti- competitive landscape." Search doesn't require a significant investment or breaking a contract to switch providers, he said. "The cost of switching is zero." -- Andrew Feinberg

28 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 29, 2008 Tuesday

LENGTH: 421 words**HEADLINE:** Social Media Increasingly a Corporate Solution**BODY:**

Major corporations are embracing social networking systems in internal and external ways. Unlike popular online social networks like Facebook and MySpace, this rapidly growing industry lets the company stay in control. Systems are being built to allow far-flung groups of employees to share institutional knowledge as well as to build and maintain corporate culture.

Many corporations are fitting their intranets with social media tools, said Ross Johnston, vice president of business development at Dotster, which sells corporate social software. Popular additions include internal profiles like Facebook's or MySpace's and discussion forums and internal chat rooms. The latter turn "one way bulletin boards for management into a conversation between all levels of the company," he said. General Electric, which Johnston called the "gold standard" for using social media internally, has seen massive growth in intranet use and employee comment, he said, citing anecdotal evidence and discussions among industry professionals.

Social tools can be especially useful in perpetuating institutional memory as the baby-boom generation leaves the workforce and younger workers take time off to start families or for other reasons. A March study by Gartner found that within five years 40 percent of Dow Chemical's employees will be of retirement age, ready to join the 40,000 Dow alumni. A large percentage of "very loyal" retirees worked for Dow their entire careers and indicated eagerness to remain involved with the company, the study said. A stellar program involving this group has been a mentoring program for new hires, based on a social-networking site for current and former employees.

Dow reaches out beyond retirees, the analysts wrote. Another major goal has been to keep women in the workforce after they have children. The site helps keep female workers connected to the company while on parental leave, encouraging them to stay involved in part-time or consulting roles even if they do leave the company. A job center on the site is the most popular section, the study said. The center has led to alumni being re-hired for at least 24 in-house and 40 contract positions, the study said.

Companies using social tools have gotten overwhelmingly favorable responses, Johnston said. Gartner found that Dow's site exceeded its annual growth goal within two months of launch. The "very loyal" Dow alumni show the same dedication to the alumni outreach site, with 95 percent of users becoming regular visitors. - Andrew Feinberg

29 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 28, 2008 Monday

LENGTH: 929 words**HEADLINE:** Privacy Experts Agree on Need for Protections; Debate Focuses on Transparency, Research**BODY:**

"Broad consensus" supports protecting Americans from data mining by law, said Fred Cate, distinguished professor and director of the Center for Applied Cybersecurity Research at Indiana University. The key to such a law is to identify "low hanging fruit" of agreement, he said. Among points of accord Cate cited: (1) The right to privacy is fundamental to other civil rights. (2) Data mining affects Americans' privacy. (3) Data mining and privacy can coexist. Most importantly, Cate said, is the need to get data miners to comply. "To cast aside that law is not an option," he said.

Limits on who can access information from data mining and why should be part of any law, Cate said. Those limits should require external authorization, preferably by an individual subject to Senate confirmation and politically accountable for decisions, he suggested.

Those harmed must have redress, he added. Such systems would assess harm and set compensation, he said. But the system also needs to learn from the process to avoid repeat injury, he said. Cate said these goals are attainable through "independent and rigorous oversight."

Privacy can be protected by limiting the types of technique used, said Ohio State University Law Professor Peter Swire. He distinguished individual from pattern-based matching techniques, urging a "middle ground" melding the two. Too much pattern matching without individual records involved could have a problematic "dragnet quality," Swire warned.

Reform of the 1974 Privacy Act should be a priority, said Barry Steinhardt, director of the ACLU program on technology and liberty. The law is in "desperate need of modernization," he said. Its glaring gaps include the "third party doctrine" and "routine use" exemptions, he said. And consensus is needed on oversight, he said. "Who is going to be the watchdog?" he asked.

Americans must understand data mining's power compared to that of historic surveillance techniques, said David Weitzner, co-director of the Decentralized Information Group at MIT's Computer Science and Artificial Intelligence Laboratory. Historically, surveillance involves a simple copy, but data mining has an "intrusive and revealing power" that must be characterized properly, he said. Data mining is "not new ... and it's not going away," Weitzner said. But privacy problems can be minimized by making uses "as transparent as possible," he said. Expectations of transparency should start out very high, he said.

A major bar to transparency is excessive classification, especially use of the "Sensitive Security Information" label, Steinhardt said. He told how a TSA official said to him: "We can't tell you if the metal detector only detects metal." A more transparent government is needed at all levels, he said. Steinhardt acknowledged the need to classify some data mining programs, but suggested that there also is a need for "due diligence" by "someone who is not a proponent" of the

program. Cate suggested that Congress simply appoint the Privacy and Civil Liberties Oversight Board that is in existence, and that agencies seek external advice in "more visible ways," making a comparison to corporations that have consumer advisory boards.

Mind the Gaps

Attempts at legislating privacy have tended to be compromised by demands to exempt researchers and national security or law enforcement players, the panel agreed. Data mining techniques are "policy neutral" compared to many security methods, Swire said. But "mission creep" is a major problem, as seen in implementing HIPAA during the Clinton years, he said. Weitzner said that writing a good privacy law demands compromise by researchers and law enforcement.

HIPAA shows how not to do privacy legislation, Steinhardt said. Future proposals should not have "huge holes" carved into them for national security or law enforcement purposes, as HIPAA does, he said.

Research is not immune from controversy, Swire said. Especially with data mining, researchers are "under pressure from the operational side," which is intent on preventing attacks. Swire suggested that a "firewall" between research projects and operational systems would encourage more good research into data mining applications.

Research exemptions to privacy laws are particularly perilous, Swire added. "If you have a research exemption, everything wants to be research," he said. People need "an overall sense of trust" that researchers will use their information responsibly, Weitzner said, invoking the public health sector as a benchmark for developing best practices that go beyond adherence to minimal requirements.

Transparency and Trust are Ultimate Goals

People should be alerted if a data mining system is flagging them, Weitzner said. Explaining repeated stops for secondary screening and establishing avenues of redress if there is a problem can build trust and help with compliance, he suggested. Thomas Oscherwitz, chief privacy officer at ID Analytics, Inc., agreed: "People need to understand the model - why am I being checked?"

Offering redress enhances trust, Cate said. Most people don't use such mechanisms, but knowing of their availability is a comfort, he said. Steinhardt cited the no-fly list, from which there is no escape. He emphasized the need for "genuine due process" in any redress system, which he said should be run by an "independent arbiter." Swire agreed, criticizing the secrecy endemic to the current process as "security through obscurity." Fans of keeping processes secret fool themselves, Swire said. "If you think ... it's a secret, you're wrong." - Andrew Feinberg

31 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 25, 2008 Friday

LENGTH: 535 words**HEADLINE:** ISPs and Lawmakers Clash on Online Safety**BODY:**

Parents and law enforcement need additional tools and resources, not more laws, to keep children safe online, Verizon Director of Technology Michael McKeehan said at a briefing Thursday held by the Latino Leaders Network. McKeehan praised a Virginia state effort to require online safety education in schools but called it an unfunded mandate, saying that more financial resources must be devoted to the problem.

More federal laws are needed when state laws don't apply, said Mercedes Salem, legislative counsel to Rep. Linda Sanchez, D-Calif., who has introduced cybersafety bills this Congress. Salem said that laws like the Megan Meier Cyberbullying Prevention Act, HR-6123, are necessary for situations "where the state can't get them," adding that "we want to send a message" on cyberstalking. Salem said the rise of social networks like MySpace and Facebook had inflamed the problem.

Parents and kids share responsibility for learning about proper conduct online, said National Center for Missing and Exploited Children online safety director Nancy McBride. She said the results of a study released Tuesday by the center and Cox Communications (WID July 23 p2) signaled "good news," and that kids and parents are becoming savvier about what they post and where.

Parents must maintain control, McBride said in response to a question about whether parents should have their children's passwords. Children "have no right to privacy online," she said. Parents need to take responsibility, she said. "Ignorance is no excuse."

Release of an Internet Safety Technical Task Force report on tools to protect children online will probably be delayed until the first quarter of 2009, McKeehan said. The task force, based at Harvard University's Berkman Center and set up under an agreement among ISPs, online social networks and the National Association of Attorneys General, is taking longer than expected to complete its report, McKeehan said.

Verizon's blocking of all but the "big eight" Usenet hierarchies (WID June 25 p6) affects only a "small number" of users, McKeehan said. The blocking is a key part of a "code of conduct" between Verizon and New York Attorney General Andrew Cuomo. (See separate report in this issue.) McKeehan said the "moderated" nature of the "big eight" groups, and the belief that the "alt" hierarchy Verizon blocked contained mostly child pornography and pirated content, were legitimate reasons for blocking them. Verizon has gone the farthest in blocking newsgroups of any ISP in a Cuomo agreement.

Cuomo's threatened lawsuit against Comcast "appears more like he is taking a position other state AGs are not following," said Family Online Safety Institute CEO Stephen Balkam. He said that though Cuomo may be "trying to be helpful," the small number of Comcast users in New York made him curious about Cuomo's actions.

Seniors' safety is a growing concern, McKeehan said, based on the growing number of elderly that he sees fall victim to phishing scams. "It's amazing how many click" on phony e-mail offers, McKeehan said, suggesting that the problem would only grow as time goes on. "Let's not neglect seniors" when it comes to online safety, he urged the audience. -- Andrew Feinberg

33 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 24, 2008 Thursday

LENGTH: 463 words**HEADLINE:** Facebook, MySpace Duel over Data Portability Efforts**BODY:**

Social networks Facebook and MySpace introduced competing sets of features a day apart. MySpace offered an open-data portability standard to allow Internet users access to multiple services without re-entering personal information or remembering a number of logins. Facebook played down portability, instead announcing an array of proprietary features to extend the site's reach -- a social-networking rehashing of the PC and Mac wars.

MySpace threw the first punch, joining industry players, including Microsoft and Yahoo, announcing support late Tuesday for the shared identity system OpenID. MySpace will offer users OpenID identifiers, allowing each to have a single sign-on recognized by many Web services. MySpace announced June 26 specifications of its data portability project, Data Availability, that similarly uses an existing standard called OAuth to let users link other services back to their MySpace accounts. By adopting OpenID, MySpace becomes the second largest provider, after Yahoo. With Wednesday's announcement, over a half billion Internet users will have access to OpenID services. MySpace at this point is only issuing users OpenID credentials, but the company said it planned to accept credentials from other OpenID providers in the near future.

Facebook CEO Mark Zuckerberg hit back late Wednesday in a keynote at the F8 developer conference in Palo Alto, Calif. He announced Facebook Connect, which he said would allow users to share their information across the Web while maintaining control of the data wherever they use it. In contrast to MySpace's adoption of OpenID and OAuth, Facebook Connect will be a proprietary system, including the site's current privacy controls. It allows other sites to incorporate Facebook features into their design and put user data back into Facebook.

Both moves drew praise from privacy advocates and other industry observers. Both feature sets are a victory for free markets, said the Progress and Freedom Foundation's Beren Szoka. Szoka called the OpenID rollout a "good example of competitive forces in the marketplace," predicting data portability will succeed as long as companies offer it responsibly. The differing approaches are "all about competition," Szoka said. Because MySpace is backed by News Corp., it has more freedom to take risks and allow more access to user data, Szoka said, but Facebook may still be reeling from last year's Beacon controversy (WID Dec 6 p3) and therefore may want to tread more carefully by maintaining control. FastCompany.tv's Robert Scoble, Microsoft's original in-house blogger and a longtime data portability advocate, told us he uses more than 30 Web services, and "any direction that gives me more access to my data and links systems together is great." - Andrew Feinberg

35 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

July 23, 2008 Wednesday

LENGTH: 253 words

HEADLINE: Adelstein Seeks Vote on Interactive Ads, Pushes 'Aggressive Family Agenda'

BODY:

A vote on banning interactive ads aimed at children is long overdue, Commissioner Jonathan Adelstein said Tuesday at the Cox Tween Summit. Adelstein worries about how "invasive" targeted and behavioral ads affect children, he said. Warning parents about marketers who spend "countless hours trying to get inside our kids' minds," he said, "We should be just as smart and aggressive in trying to keep them out."

Adelstein urged a vote on a proceeding to ban interactive ads in children's programming, stressing the need to protect kids from exposure to ads via interactive TV platforms. "It's time that we act," he said, urging that the FCC clarify an existing ban on ads in children's programming that include embedded content. He and colleagues have concurred for some time on a "tentative conclusion" regarding the interactive ad ban, he indicated to us, but would not say if or when a vote will occur.

The FCC can use its authority to exert positive influence on the online space, Adelstein said. Besides addressing ad rules, he offered an "aggressive family agenda" for the FCC. This included urging a proceeding on "advanced blocking techniques," and an en banc summit on protecting America's children.

FCC action can "put wind in our sails" for other areas of concern, Adelstein said. Setting standards for traditional media could blaze a trail for the Internet industry's efforts, he said, and lead Congress to pass comprehensive privacy laws protecting not only children, but all Americans, he said. - Andrew Feinberg

37 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 23, 2008 Wednesday

LENGTH: 315 words

HEADLINE: Court Says Child Protection Law Violates First, Fifth Amendments

BODY:

The 1998 Child Online Protection Act is unconstitutional on both First and Fifth Amendment grounds, a three-judge panel said Tuesday, upholding a lower court judge's March 2007 ruling. Also upheld by the 3rd U.S. Appeals Court in Philadelphia was the same panel's previous decision overturning the law on several different grounds (WID March 23/07 p1). Writing for a unanimous panel and rejecting a number of government arguments, while making myriad references to the panel's prior decisions, Judge Morton Greenberg wrote that the law is unconstitutional because it "cannot withstand a strict scrutiny, vagueness, or overbreadth analysis." The law seeks to shield children from exposure to online pornography.

The history of the case known as *ACLU v. Mukasey* can be traced to a 1998 lawsuit filed the day after COPA became law. The Supreme Court heard the case on appeal in 2002, ordering a new trial to determine the usefulness of new content filtering technology and whether or not such technology was more useful for protecting minors than enforcing COPA would be. After a second trial, in 2007, the law was overturned a second time in a decision appealed to the same 3rd Circuit panel. That led to Tuesday's ruling, which the government could appeal once again to the Supreme Court.

The government has spent 12 years fighting the ACLU in Internet pornography litigation, the Center for Democracy in Technology said in a news release lauding the decision and calling the government strategy "an utter failure." CDT Senior Counsel John Morris, lead attorney in the 1997 *Reno v. ACLU* case, said the 3rd Circuit's latest decision "empowers parents, respects the First Amendment and acknowledges the diverse sensibilities of American families." No statement was available at our deadline from the office of U.S. Attorney General Michael Mukasey or the Department of Justice. - Andrew Feinberg

38 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 23, 2008 Wednesday

LENGTH: 404 words**HEADLINE:** Adelstein Seeks Vote on Interactive Ads, Pushes 'Aggressive Family Agenda'**BODY:**

A vote on banning interactive ads aimed at children is long overdue, FCC Commissioner Jonathan Adelstein said Tuesday at the Cox Tween Summit. Adelstein worries about how "invasive" targeted and behavioral ads affect children, he said. Warning parents about marketers who spend "countless hours trying to get inside our kids' minds," he said, "We should be just as smart and aggressive in trying to keep them out." Commissioner Deborah Tate said in brief remarks that the "unbelievable opportunities" of broadband pose challenges that can't be solved by "government regulation." There needs to be "a conversation between caregivers of all types," she said.

Efforts to protect children online are hamstrung by lawmakers and courts obsessed with constitutionality, said child advocate and TV personality John Walsh. Law enforcement constantly is hampered by courts "bogged down in the First Amendment," he said. He strongly criticized *Ashcroft v. The Free Speech Coalition*, the 2002 overturn of a ban on computer-generated child porn, saying even animation depicting such acts should be illegal. Walsh did not appear aware of Tuesday's decision by the 3rd U.S. Appeals Court in Philadelphia to overturn the 1998 Child Online Protection Act on both First and Fifth Amendment grounds. (See separate report in this issue.)

Adelstein urged a vote on a proceeding to ban interactive ads in children's programming, stressing the need to protect kids from exposure to ads via interactive TV platforms. "It's time that we act," he said, urging that the FCC clarify an existing ban on ads in children's programming that include embedded content. He and colleagues have concurred for some time on a "tentative conclusion" regarding the interactive ad ban, he indicated to us, but would not say if or when a vote will occur.

The FCC can use its authority to exert positive influence on the online space, Adelstein said. Besides addressing ad rules, he offered an "aggressive family agenda" for the FCC. This included urging a proceeding on "advanced blocking techniques," and an en banc summit on protecting America's children.

FCC action can "put wind in our sails" for other areas of concern, Adelstein said. Setting standards for traditional media could blaze a trail for the Internet industry's efforts, he said, and lead Congress to pass comprehensive privacy laws protecting not only children, but all Americans, he said. - Andrew Feinberg

40 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 18, 2008 Friday

LENGTH: 456 words**HEADLINE:** Cable's Child-Porn Attack Targets 'Worst of Worst'**BODY:**

Cable Internet providers have agreed to check up and report back on Web sites that the National Center for Missing and Exploited Children says are distributors of child pornography. The center and the NCTA announced an agreement Thursday, which was obtained by Washington Internet Daily.

Within 90 days, network operators will receive a list of sites identified by the center. They will check whether the sites on their networks offer child pornography. If they do, the operators will block access and tell the Center. ISPs aren't to turn in users. Only the center will have contact with law enforcement, under the agreement.

The agreement is the result of negotiations prompted by the NCTA, said a letter from Rhode Island Attorney General Patrick Lynch, the president of the National Association of Attorneys General. He called the deal "unprecedented" and said the agreement would "limit the ability of predators to store and exchange images of exploitation of... the most vulnerable in society."

The accord will build on the cable industry's commitment to online safety, said NCTA President Kyle McSillarow. The operators taking part are "reaffirming their strong commitment to online safety... for all American families."

Thursday's announcement drew praise from all sides. FCC Commissioner Robert McDowell said he was "delighted." Sen. Ted Stevens, R-Alaska, the Commerce Committee's ranking member, called it "an important step in combating online child pornography." He said much more work is needed to educate children about online safety.

The Center's president, Ernie Allen, told us he too was pleased with the outcome of talks with the NCTA. He called the agreement a "reasonable and balanced approach, within the law and constitution." Allen said the pact is meant to "select the worst of the worst" for prosecution. He compared it to successful efforts across Europe, the U.K. and Canada, saying it provides "proactive process" singling out only clearly illegal material.

Staunch privacy advocates were mostly pleased with the agreement. Center for Democracy and Technology counsel John Morris said it raises only two possible problems. He said bills in Congress, notably the SAFE Act of 2007 (HR-2791), could turn the Center's list into a "government-sanctioned blacklist." And though the Center is required to make additions to the list, there's no provision in the agreement that provides for removal of sites from the list if they no longer host illegal content. Allen assured us that the list is checked for accuracy and revised on a daily basis. Morris said he still was worried about ISPs' use of old lists. Lawfully-operating sites could get caught up in the system, raising "significant concerns," he said. - Andrew Feinberg

42 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 17, 2008 Thursday

LENGTH: 283 words

HEADLINE: NPR Reaps Gains from Internet, Social Media Presence Push

BODY:

National Public Radio is expanding its Internet presence to connect with its audience and improve programming. Though not a new development, the quietly ramped-up efforts have drawn a massive positive response, said Andy Carvin, senior product manager for community.

Carvin has evolved into a "strategist for social media" since joining NPR in September 2006. NPR had blogs and discussion forums when he joined, but Carvin's job has been to look for ways to use Web technologies, social media and online communities to further NPR's mission by helping form "a more constructive relationship with the public," he said.

Carvin's first task was to find ways to use social media to make NPR programs "more vibrant," he said. He cited as a success NPR's Tell Me More, which arose from NPR Rough Cuts, a concept in which the show had a blog and podcast before it went on the air, Carvin said.

Another Carvin project, "Get My Vote," lets listeners record, upload and tag "op-eds" that NPR shows like Talk of the Nation and Weekend Edition Sunday have used to "generate a dialogue with the public," he said.

The "Get My Vote" concept and platform have been adopted by at least one station, KPBS(FM) San Diego, Carvin said. KPBS uses it to give listeners an outlet for commentaries on local candidates, he said. "Because NPR is still a member organization - it is important for these tools to be able to be localized... for member communities."

NPR shows Talk of the Nation, Bryant Park Project and others have solicited feedback directly using blogs and even microblogging service Twitter, Carvin said. This lets listeners offer feedback even if they can't call in and get on the air, he said. -- Andrew Feinberg

44 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 16, 2008 Wednesday

LENGTH: 748 words**HEADLINE:** Microsoft Cries 'Monopoly' on Google-Yahoo; Icahn Intrigue Could Bring More Hearings**BODY:**

Google and Yahoo can partner and the search advertising market still can be competitive, senators heard at a Tuesday Antitrust Subcommittee hearing. At the outset, Chairman Herb Kohl, D-Wis., said he wonders if implementing the proposed Yahoo-Google agreement would "reduce Yahoo to nothing more than the newest satellite in the Google orbit."

If Google doesn't already have a monopoly, a Google-Yahoo partnership certainly would create one, said Microsoft General Counsel Brad Smith. Softpedaling his company's repeated attempts to buy Yahoo, Smith said that in addition to price-fixing problems posed by the deal, the combined 90 percent market share that the Google and Yahoo search engines enjoy would enable the combined company to collect unprecedented amounts of user data. "We will have a national privacy policy," Smith said. "It will be Google's privacy policy."

The proposal offers a non-exclusive commercial arrangement that will protect competition and spur innovation, said Google Chief Legal Officer David Drummond. Under it, Yahoo could offer advertisers more benefits yet still compete as a search engine, he said.

Each company is moving to address privacy and pricing concerns, Drummond said. Yahoo will anonymize search user IP addresses before passing queries to Google, and Google will erect a "privacy firewall" to bar exchange of real-time pricing data between the companies and limit disclosure of information when a Yahoo search user clicks through a Google-supplied ad. These steps "demonstrate how vigorously the companies plan to continue competing against one another," he said. He contrasted that with Microsoft's attempts to buy Yahoo outright. He said Yahoo could reinvest revenue from the Google partnership into its own platform.

The "commercial arrangement" would "help make our company an even stronger competitor to Google, to Microsoft, and to others," Yahoo General Counsel Michael Callahan told the subcommittee. Yahoo would maintain its own search algorithms and ad sales platform and "will continue to do everything we can to grow our share and also strengthen our competitiveness in search advertising," even against Google, Callahan said. "We have every intention of fighting them and winning, in this and other areas," he said.

The hearing got tense when Smith brought up Microsoft's June meeting with Yahoo at the San Jose airport, saying that Yahoo CEO Jerry Yang had called the search advertising market "bipolar," with Google on one end, and Microsoft and Yahoo together on the other. Kohl reminded Smith that he was testifying under oath and asked if those were Yang's words. Smith said yes. Callahan interjected, noting that he was a participant in the meeting. He didn't directly address Smith's characterization of Yang's remarks, but said of the meeting, Yahoo's board had "made a conscious decision to stay in search" and compete against Google and Microsoft as an independent company.

Microsoft Cries 'Monopoly' on Google-Yahoo; Icahn Intrigue Could Bring More Hearings WASHINGTON
INTERNET DAILY July 16, 2008 Wednesday

At one point, Smith suggested that DoJ's review of the deal indicated its illegality. But Callahan and Drummond said that the companies requested the review, and that, considering Microsoft's possible involvement in the proxy fight being waged by activist investor Carl Icahn, the department scrutiny was more than welcome.

Ranking Member Arlen Specter, R-Pa., asked Smith about the scope of recent Microsoft actions involving Icahn's proxy fight. Smith demurred, calling that a "fluid situation." Specter interrupted: "If Icahn wins, doesn't Microsoft get Yahoo?" Repeatedly pressing Smith, Specter suggested the possible need for another hearing on the matter. Kohl asked Smith "flat-out" if Microsoft opposes the deal out of desire to acquire Yahoo, wondering aloud if that wouldn't be just as anticompetitive. Microsoft has been "strongly interested in... some kind of important transaction with Yahoo," Smith said, adding that a Microsoft-Yahoo combination would align "a critical mass... by putting a small number two and an even smaller number three together."

When we asked about Microsoft's relationship with Icahn, which a senator termed "hand in glove," Smith said Microsoft would comment only in accordance with SEC rules on proxy statements, referring us to a news release issued this week. Drummond wouldn't say whether Microsoft and Icahn acted in good or bad faith. The events look "a little odd," he said. "It seems like there is a concerted campaign against Yahoo to drive the price down in order to get a better price." -- Andrew Feinberg

48 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 11, 2008 Friday
Correction Appended

LENGTH: 397 words

HEADLINE: Senate Not Conflicted over Members' Online Video

BODY:

As some House members debate rules for their use of online video (WID June 10 p4), Senate discussion of the same topic has been much quieter. The Senate Rules Committee, chaired by Sen. Dianne Feinstein, D-Calif., has been working quietly to open the door to new technologies by updating rules last revised in 2000, said Staff Director Howard Gantman.

The surge of new Internet technologies offers offices ways to "better communicate with the public and increase the transparency of government operations," Gantman said. As chairman, Feinstein "has sought on a bipartisan basis to open the door to these new technologies" and believes that "it is time the Senate moves into the modern era," he said.

The committee has talked with YouTube, main focus of Senators' questions and concerns, and the video sharing site is creating a special "channel" for Senate content so commercial or political content won't mix with official videos. Members still can use their own resources to post videos and participate personally online, he said.

Some senators worry about outside sites using data mining technology to track viewers of official videos hosted off the senate.gov domain, Gantman said. The committee kept a ban on data-mining the official domain because YouTube has agreed to not track or log such data, he explained. Unlike the heated back-and-forth dominating the House debate, Feinstein and Bennett are working toward what they expect to be a unanimous agreement among committee members, Gantman said.

But new rules, restrictions, and "white-lists" of sites where House members may post videos may not apply to a video site adopted by Rep. John Culberson, R-Texas, for publishing live videos from his mobile phone. Fears voiced by Rep. Michael Capuano, D-Mass., of mixing of official and political content are unfounded, Qik CEO Bhaskar Roy said Thursday. Not only does Qik host only user-generated content, but a user's individual account page contains no links to unrelated videos unless specifically placed by the user, Roy said. There is "absolutely no possibility" of an unsuspecting viewer finding an official video next to a political ad if the member is following the rules, he said. Qik has a feature with which official House member pages could link together to keep that content separate from other accounts, Roy said, and Qik doesn't host ads of any kind. -- Andrew Feinberg

CORRECTION-DATE: July 15, 2008

CORRECTION:

Bhaskar Roy is a co-founder, not CEO, of Qik.com (WID July 11 p2).

49 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 11, 2008 Friday

LENGTH: 441 words**HEADLINE:** Barton Optimistic on Health IT Bill's Chances, Wants Privacy Protection**BODY:**

Health IT legislation being drafted must help consumers understand their privacy rights, not conditioning them to sign away those rights, House Commerce Committee Ranking Member Joe Barton, R-Texas, said Thursday at a "Privacy in the Internet Age" event sponsored by CQ and Dow Lohnes. The bill will hopefully be ready for mark-up within two weeks, he said, add that privacy will be paramount in the measure. "Nobody in the world has a right to know anything about me unless I want you to -- period," he said.

The bill would represent a major improvement over previous health privacy laws like HIPAA, Barton said. Disclosure requirements aren't adequate for evolving technologies or consumer protections, he said, saying that any bill should allow patients to limit disclosures to "what other people need know to provide you health care." Exchanges of information are necessary but should be limited, he said. "If someone wants to collect the entire data set... I've gotta be asked."

The bill will have "the strongest privacy protection... of any bill that's gone through the House or the Senate in the past five or 10 years," Barton said. Its success will hinge on how it defines privacy, a step now subject to "active debate," he said. Barton boiled it down: "I want to be the gatekeeper for what everybody else knows about me... It's not a legal definition, but it works." He said he isn't sure how the committee will define privacy. Echoing Supreme Court Justice Potter Stewart on pornography, Barton said, "I know it when I see it."

Barton sees no privacy distinction between electronic health records, equivalent to patient "charts," and personal health records, which patients can maintain themselves and store in commercial systems like those planned by Google, Microsoft and others, he said. His view of privacy doesn't vary by the medium or method of storage, he said.

The bill will lack HIPAA's many loopholes and confusing wording, Barton said. Most people realize that in the age of the Internet they don't have automatic privacy. Because of this, Barton was adamant that "there are not going to be exceptions" like the ones in previously enacted legislation, he said.

Barton expects the bill to be set for markup within weeks, he said, adding that he's confident it will quickly move to a House floor vote, and will pass easily. The outcome, while an improvement, won't please everyone, he warned. "We're gonna get a good bill, with good privacy protection, but it's not gonna be perfect." Privacy will improve as the law is carried out and lessons are learned, he said. "Over time we'll get there. This is our first stop." -- Andrew Feinberg

52 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 10, 2008 Thursday

LENGTH: 661 words**HEADLINE:** Web Proposal for House Sparks Revolt**BODY:**

Members on both sides of the aisle oppose proposed revisions to rules governing House members' Web sites (WID July 9 p2).

Several prominent Republicans Wednesday criticized a pending proposal to revise guidelines for how members post Internet content as an attempt at censorship. The proposal would "shut down what has emerged as a free and helpfully uncensored pipeline of real-time information between the American people and their elected leaders," said House Minority Leader John Boehner of Ohio. House Franking Commission Chair Michael Capuano, D-Mass., who authored the proposal, said he was trying to modernize the rules while preventing commercialism.

Boehner sent a strongly worded letter Wednesday to House Speaker Nancy Pelosi, D-Calif., criticizing the proposal for limiting postings only to services "approved" by the Administration Committee. He said members should be able to use services they believe "will best assist them in communicating with their constituents." He also said members should be free to use any service on the same terms that anyone else could use them. "We must encourage, not restrict the free and open flow of uncensored information between the American people and their elected leaders over the Internet," Boehner said.

An alert by Rep. John Culberson, R-Texas, galvanized "social media" interests. By 11:59 p.m. Tuesday, a site built by Aaron Brazell, a Baltimore social-media consultant, had collected a list of over 40 blog posts, with authors from across the political spectrum, decrying Capuano's proposal. Brazell told Washington Internet Daily that "what happened last night was not partisan," and said his motivation came from a belief that "Congress... should be making every attempt to find the best way to communicate with the public." Brazell said many people communicate online using new social media tools such as those under discussion. "Why shouldn't Congress be able to do the same?" he asked.

Culberson backed away from his initial anger over the issue, during an interview Wednesday. He said what troubled him was that the proposed rule would "for the first time, regulate the Internet and the ability of members of Congress to utilize the Internet."

Culberson acknowledged the validity of some restrictions on congressional Web use, such as those separating official business from campaigns, and said he had made inquiries about how to follow the rules while using cutting edge technologies. He said the Administration Committee told him that "no one had ever asked before" and until recently no one had objected.

Though Culberson declined to call the Capuano proposal an attempt at censorship, he bristled at the idea that he would have to receive approval to communicate as he wanted. The Administration Committee's efforts, he said, were akin to "King Canute trying to stop the tide" and said that he would approach Capuano "in a nonpartisan, friendly way"

Thursday to resolve the dispute. Culberson said he plans to continue his Web video postings regardless of any rule changes. "This technology is allowing us to really shine sunlight into the federal government... For me, it's tremendously exciting."

Capuano may not be ready for compromise. "I guess they don't care if constituents clicking on their videos will be treated to commercials for anything you can imagine, from the latest Hollywood blockbuster to Viagra," Capuano said in a written statement. He acknowledged that ads are easily identifiable and said avoiding the perception of impropriety was the goal of his proposal. "Members of Congress who use taxpayer money to communicate with constituents should be held to the highest possible standard of independence -- and the appearance of independence."

Culberson said that instead of regulations, the committee should trust members' judgment. "Obviously, I'm not going to use official resources to get people to go to a Web site that says 'vote for me.' That's against the law." - Andrew Feinberg

54 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 09, 2008 Wednesday

LENGTH: 469 words**HEADLINE:** GOP Upset with Rule Proposal on Web Video Posts**BODY:**

Republican leaders are upset with a proposed House rule that would set limits on congressional office posting of videos and other content on the Internet, Minority Leader John Boehner of Ohio said Tuesday. "House Democrats... seem to want to wall themselves off from scrutiny by American citizens," said Nick Schaper, Boehner's director of new media.

The rule could curtail members' use of online tools to produce video and communicate with constituents, Boehner said. House Franking Commission Chairman Michael Capuano, D- Mass., outlined the proposal in a June 24 letter sent to House Administration Committee Chairman Kevin Brady, D-Pa. Capuano's letter suggested several revisions to the rules governing how members could post video and other content to the Web. It suggested that content not be posted on a site where it may appear with commercial or political information or any other information not in compliance with the House's content guidelines. The proposal also suggested that content be restricted to sites on a pre-approved list the House Administration Committee would maintain.

The proposal upset some members. Reps. Vern Ehlers, R- Mich., Kevin McCarthy, R-Calif., and Tom Price, R-Ga., sent Capuano a letter June 25 suggesting that members be able to use Web technologies to post content as long it complies with "House rules and franking content regulations." Their letter also suggested that members be allowed to use free communications and networking services as long as the services are available on equal terms to all members.

Schaper said the proposal amounts to censorship, adding that House Republicans want all members have the freedom to use the "most advanced tools possible to ensure they're communicating with their constituents."

Capuano said the Republicans "would rather operate without rules and open the House to commercialism," in an e-mail to us. Capuano denied any attempt to censor the types of messages or content that members could post, and said his proposal "allows the American public to have full access to information from Members while ensuring that taxpayer dollars do not support commercial or political advertising on the web."

The Administration Committee doesn't have any specific text drafted for revising the rule, said a committee spokesman, but added the committee expects to take action before Congress recesses at the end of the month.

Rep. John Culberson, R-Texas, who has started to use many of these new technologies with great enthusiasm (WID July 1 p3), alerted supporters Tuesday afternoon by posting on his Twitter page. He said the Democrats' proposal would require "prior approval of all posts to any public social media/internet/www site by any member of Congress." Culberson said the rules were "outrageous" and vowed to fight them. - Andrew Feinberg

56 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

July 08, 2008 Tuesday

LENGTH: 376 words**HEADLINE:** Convergence of Web 2.0, Wireless Boost Communication in Emergencies**BODY:**

San Diego residents losing mobile phone voice service while fleeing last year's wildfires turned to those devices' text functions, which use separate channels and remained in service, and especially the text-based microblogging service Twitter, which resembles a form of instant messaging for mobile. By posting their "status" to the service, they let friends and family know their locations and enabled authorities to monitor the fires more quickly.

Such services can help first responders find those in need and help people keep in touch, security consultant David Stephenson said in a blog post citing the advent of location based services, camera and GPS-equipped phones and Web 2.0 services.

The Department of Homeland Security and CTIA's Wireless Foundation saw the post and asked Stephenson to consult on the new technology. The foundation soon will report on emergency preparedness, a paper largely based on Stephenson's findings, said Executive Director David Diggs.

Pictures taken by citizens using GPS-enabled phones and uploaded to Yahoo's Flickr service tagged "LAFD" enabled the Los Angeles Fire Department to see where the fire was headed, spokesman Brian Humphrey said. Humphrey said the department also monitors and uses Twitter to spread information and stay in touch with communities it serves.

Natural disasters aren't the topics covered with "2.0" tools. Qik CEO Bhaskar Roy said his service, which allows live streaming of video from mobile phones, recently saw use "on a local, small scale" by people to tag and broadcast live views of traffic accident scenes. That lets commuters check routes before leaving the office, and sometimes see events live on mobile phones. When Seismic CEO Loic le Meur and FastCompany.tv videoblogger Robert Scoble were in an accident en route to a Los Angeles conference, Scoble used his Qik camera to film the other driver before he drove off, enabling police to track him down, Scoble later said.

Professionals also use the new tools. Assigned to the White House in December, network news camera operator Jim Long saw smoke at the Eisenhower Old Executive Office Building. Ordering his camera live feed picked up on the air, he used his BlackBerry to let Twitter friends see the news. --- Andrew Feinberg

60 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 07, 2008 Monday

LENGTH: 367 words

HEADLINE: Public TV Online Could Alter PBS Fortunes, Widen Audience

BODY:

PBS plans to expand online video offerings to tap potential revenue streams and draw younger viewers to local stations, said Vice President vice Andrew Russell of PBS Ventures. The rise in video downloading and sharing, including content on PBS.org, has become "a very big part of the story," Russell said.

PBS uses two main content distribution channels. One is a "download to own" model, like Apple's iTunes service, said Russell. The first prong of PBS' online strategy, this came into use about two years ago, he said.

A second front opened in December -- partnerships with video sharing sites with embedded advertising. Sharing site Joost launched in December, with YouTube following in January. Hulu, the joint NBC-Universal-Fox venture, became a partner last week, Russell said. Two original "download to own" ventures changed models to be advertiser-supported.

Ad revenue is not significant, and viewership varies weekly depending on whether content is hosted on PBS.org or on a member station's site, Russell said. He described the work as "very experimental, adding that with expanded viewership ad revenue will grow appropriately.

Downloads are proving far more lucrative. PBS has had great success with iTunes, and with a new formula for gauging producer income shares, Russell said. He hopes to draw more producers to work with PBS as a distribution channel for their programming, he said.

The most popular programs by far have been science and children's programming, especially those made part of iTunes "Green Room" area. Warship documentary "Carrier" did "very well," Russell said, with the free preview episode on iTunes leading many customers to buy the series.

But the ultimate goal remains to improve the station member-supported model, Russell said. He emphasized every "free" video includes multiple messages stressing local stations' importance and encouraging viewers to ask local stations about joining. PBS hopes to use the Internet to "evolve and strengthen the member-station relationship" and offer member stations more programming, he said. "As we see the space mature... what you will have is an audience with a broader taste for different kinds of programming." -- Andrew Feinberg

61 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 07, 2008 Monday

LENGTH: 462 words**HEADLINE:** Social Networking Giants Take Opposing Tacks in China**BODY:**

Facebook's new Chinese language translation comes with no new policy for dealing with China's government, it said. The Chinese version of the social networking Web site and platform quietly launched last month. CEO Mark Zuckerberg had said his company had reservations about such an expansion (WID June 10 P5).

"We believe that people around the world should be able to use Facebook to communicate and share information with their friends, family and coworkers, regardless where they live or what language they speak," Chief Privacy Officer Chris Kelly said in a written statement.

Facebook's policy is to "evaluate formal data requests from government entities on a case-by-case basis," and the company won't release data to authorities "until we have the good faith belief that we are legally obligated to do so," Kelly said. That standard hinges on the authorities' getting a court order or using another lawful process, said an official familiar with the company's China strategy. The official voiced doubt that Facebook ever would have to validate a legal process, saying Chinese authorities seeking information are unlikely to use legal maneuvers. But if a Chinese court order meets Mutual Legal Assistance Treaty requirements, the official said, Facebook would "probably comply with it like we would with any other country." That possibility is only hypothetical, the official added.

Facebook's policy "seems very optimistic," said Eddan Katz, a Yale Law School lecturer and the Electronic Frontier Foundations' international affairs director. In recent years China's legal system has accumulated a body of case law on the government's authority to obtain information, he said. Facebook's stated position is "insufficient," Katz said. It doesn't make clear which country's law Facebook would follow, he said, and even under U.S. law, "there are ways in which information can be gathered... that people would feel uncomfortable with," he said.

Katz praised some recent Facebook attempts to clarify its privacy policies. But he said Kelly's statement "is not necessarily in conformity with consumer expectations," because of its vagueness. Facebook's situation requires a policy "beyond saying they'll be true to the letter of the law," he said: "There needs to be clarification of which law, under what circumstances."

MySpace's position differs dramatically from its rival's. Rather than endure the pressures and challenges of being an American company operating under Chinese law, MySpace licensed its brand and technology to a Chinese-owned company that runs a version of the site. A company official said MySpace China is a "locally owned, operated and managed Chinese company that runs MySpace.cn and functions like any Chinese Internet company would." - Andrew Feinberg

63 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 03, 2008 Thursday

LENGTH: 299 words

HEADLINE: Task Force Experts to Study Child-Protection Technologies

BODY:

The Internet Safety Technical Task Force wants to study tools offered to protect children online. The group was convened as part of MySpace's agreement with 49 state attorneys general to further protect children online (WID Jan 15 p1). Based at Harvard University's Berkman Center, the group includes Comcast, Facebook, Microsoft and the National Center for Missing and Exploited Children among others.

In a Wednesday request for proposals, the group's Technical Advisory Board invited submissions on "technologies relevant to child safety online," for a "thorough review" of whether they: (1) Limit harmful contact between adults and minors. (2) Limit harmful contact between minors. (3) Limit or prevent minors from accessing or creating inappropriate content on the Internet. (4) Limit availability of illegal content on the Internet. (5) Keep minors from accessing particular sites without their parents' consent. (6) Prevent harassment, unwanted solicitation and bullying of minors on the Internet.

The submission template strongly suggests use of an ACM/IEEE format "in both style and substance" to ensure scientific rigor, officials said. In its review, the advisory board will look at the extent to which the technology depends on law and public policy. "We are looking for technical solutions that can have impact right now, as well as tools that show future promise," Task force director and Harvard Law Prof. John Palfrey said.

Technologies on the board's target list include "filtering, blocking, parental controls, labeling, rating, identification, authentication, age verification, imaging, search and forensics," the request said. Submissions are due July 21. It will present its findings in the final report of the Internet Safety Task Force, due out late this year. - Andrew Feinberg

65 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

July 01, 2008 Tuesday

LENGTH: 520 words**HEADLINE:** DNC Tack Could Level Playing Field for Internet Companies**BODY:**

Democratic National Committee refusal of PAC and lobbyist money could level the playing field for Internet companies' lobbying campaigns by removing advantages held by telcos, entertainment firms and other big spenders, officials said. But a "trickle-down" effect to House and Senate races will take time, they said.

In politics, technology companies are all over the map, unlike industries historically aligned with one party or another. For example, since a 1998 antitrust lawsuit drove it to lobby more energetically, Microsoft has split its political contributions relatively evenly between the major parties. In contrast, Google almost exclusively has donated massively to Democrats. Meanwhile Internet industry political efforts nearly always have been outflanked financially by more established, deeper-pocketed sectors like telecommunications and entertainment, officials said.

Removing money from the political chessboard leaves technology companies no worse off, said Lawrence Lessig, the Stanford University law professor and founder of Change Congress: "Silicon Valley has been very bad at... leveraging financial resources." Instead, Lessig suggested, lessening PAC and lobbyist financial sway with the Democrats assures that "the playing field is about ideas, not about money."

Lessig is less optimistic about House and Senate candidates doing as the DNC has, he said. "I haven't yet seen that the party, as opposed to Obama, has the same view about this," he said. A strategy of small contributions will have a harder time working its way "down the political chain," he added.

"You're not going to rebuild the system in a day," agreed veteran Democratic strategist Joe Trippi. Manager of John Edwards' 2008 primary campaign and Howard Dean's 2004 effort, Change Congress ally Trippi predicted that the "Obama/DNC" system could take three or four election cycles to take root. But he is optimistic that some House and Senate candidates will take the DNC pledge this campaign, he said. For a Presidential nominee and a major party to refuse PAC and lobbyist money is a "huge step in itself," whether or not the commitment flows down the ticket, Trippi said.

The DNC gesture will help the Internet industry sidestep more established players on issues like net neutrality, Trippi said. Combined with widespread political adoption of social networking tools, the DNC/Obama model could create a "greenhouse for grassroots." This could allow companies to bypass lobbyists and rally customers to get elected officials' attention rather than donate to campaigns year after year. The new model is "turning the page against the fat cats," he said. Sen. John McCain of Arizona also could adopt the policy that the Democratic party has, Trippi said: "It would be great just to see the RNC take the same pledge."

The new model won't affect Google right away, said Adam Kovacevich, senior manager for global communications and public affairs. Google's NetPAC has contributed only to individual members of Congress, not to party committees,

he said. Microsoft representatives weren't available at our deadline. - Andrew Feinberg

68 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 24, 2008 Tuesday

LENGTH: 542 words**HEADLINE:** Campaign Veterans Say Internet Use Important, can Translate to Governing**BODY:**

Presidential candidates' Internet efforts during the primary season were vastly improved compared to previous campaigns, said a group of Internet directors representing almost all of both parties' primary candidates, including the two presumptive nominees, at the Personal Democracy Forum.

Giving volunteers and staff the tools and training to effectively use the Internet has been a key factor in the Sen. Barack Obama campaign's success, said Obama Internet Director Joe Rospars. His counterpart on the Clinton campaign, Peter Daou, agreed and said Sen. Hillary Clinton's campaign had integrated Internet savvy people at every level of the campaign. McCain Internet Director Mark Soohoo said the campaign considers it "important to have a seat at the table for the Internet team." Tracy Russo, who worked on the John Edwards campaign said her team had a leg up in that the candidate's wife, Elizabeth Edwards, had the experience of being a blogger herself.

Fund-raising is often given too much importance in the overall online effort of a campaign, said Mindy Finn, who worked for the Mitt Romney campaign as director of E- strategies. Finn said she was "disappointed that most candidates still don't get the Internet as more than a fund- raising tool."

Internet advocacy and blogging have moved beyond the "netroots," the panelists said. Russo said Obama's campaign blog and the community on the site has been "incredible." Rospars and Soohoo said differences between the Obama and McCain campaign blogs are representative of their candidates' target audiences.

The Internet has allowed the 2008 campaigns to leverage offline grassroots networks, said Finn. She compared Obama's success to the Bush-Cheney 2004 campaign, which used online presence to mobilize fundraising, volunteers and get-out-the- vote efforts. When moderator Micah Sifry asked how McCain could catch up, Finn backed up a bit and discounted the importance of Internet support, saying McCain's strength lies with grassroots supporters that may not be active online. Rospars disagreed, saying the Bush-Cheney model was one that the Obama campaign was looking at, in terms of using technology to make field organizing more efficient as well as mobilizing online supporters. Daou added that online social networks like the My.BarackObama.com system are "the future of campaigns."

The discussion turned heated when Sifry asked if a campaign that successfully uses the Internet can transfer that knowledge into governing. Russo said a campaign that uses the Internet will "translate into a techno-savvy administration." Almost immediately, Soohoo, whose candidate has admitted that he doesn't use a computer, fired back that using technology isn't necessary to run a tech-savvy government, but that McCain "understands the Internet."

Daou said the Democratic runner-up can't merge her substantial e-mail list with the campaign of Democratic presumptive nominee Obama. Daou said campaign finance regulations prevented the two campaigns from merging their lists, although he would not go into detail on the specific rules in question. Instead, Daou said Clinton would use her

Campaign Veterans Say Internet Use Important, can Translate to Governing WASHINGTON INTERNET DAILY June 24, 2008 Tuesday

substantial list to "vigorously encourage" her supporters to vote for Obama in the November election. -- Andrew Feinberg

71 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 23, 2008 Monday

LENGTH: 928 words**HEADLINE:** Copyright Sent Entertainment Giants on Divergent Paths, ABA Told**BODY:**

Despite public anger and what he deems reams of media misinformation, Kenneth Doroshow, RIAA senior vice president for litigation and legal affairs, has faith in his industry's strategy of litigation to defend copyrights, he told the American Bar Association CyberLaw conference Thursday. Evidence is "quite strong" that the labels picked the right battlefield on which to defend their revenue streams, he said. And slowly but surely, despite reports otherwise, RIAA is refuting the defenses defendants most commonly use, Doroshow said.

However, film and TV generally have avoided litigation, preferring a "cooperative model," said NBC Universal Vice President for Public Policy David Green. Invoking RIAA litigation against Verizon, Green contrasted producers' new strategy with labels' "old model" of litigation, pitting copyright holders against Internet providers. The new model is apparent in positive TV and film industry ties among content providers and other parties, such as user generated content (UGC) sites like YouTube, ISPs, universities and consumer electronics and IT vendors, Green said. He compared the RIAA strategy of takedown and sue to a game of "Whac-a-Mole," suggesting the "new model" would bring about a world where "a digital ecosystem dominated by theft benefits no one."

The more conciliatory strategy arose during the breakout success of YouTube and other UGC sites, Green said. The Saturday Night Live "Lazy Sunday" video, among the first TV clips to go "viral," signaled that the "old strategy" wasn't going to work, he said. Demanding YouTube take down infringing material, NBC constructed its own site offering the same clips, bracketed with ads. That inspired other legitimate video streaming sites, including the hugely successful Hulu.com joint venture, and NBC.com.

Legal theories challenging the validity of RIAA suits have been thrown out, Doroshow said. Defenses for which he had particular scorn included claims that RIAA investigators have permission to download files, thereby invalidating the basis for claiming infringement, that major labels operate illegally as a cartel and that neither expert testimony nor evidence used by the RIAA to prove infringement are reliable. The latest defense salvo, the idea that making a file available does not constitute infringement, is simply the "flavor of the month," Doroshow said.

Make Friends, Not Defendants

Fair use does apply on UGC sites, Green acknowledged. "UGC Principles" drafted by industry leaders from both sides encourage protection of copyrights while acknowledging and respecting fair use, he said. UGC sites are starting to identify and block "watermarked" content such as wholesale uploads of entire shows rather than clips incorporated into mashups, he said. All parties, including content producers, UGC sites and consumers would benefit from adherence to the principles, Green said.

Verizon, Comcast and other ISPs entering video also stand to gain from stopping piracy, Green said. Rather than

ignite an "adversarial relationship," they have incentives to discourage piracy and filter out large video downloads. Both sides want to "convert pirates into customers" by making it easier to buy desired content than to steal it, he said. Exploring the "cooperative model" theory, he said universities offer a prime example of a working partnership. Citing Illinois State University findings that university networks see five times more uploading than downloading, Green said many universities now use filters to identify and warn students that share infringing content. Most "who get a first notice... don't get a second," he said. These partnerships should lead all parties to declare piracy to be theft while making it easier to obtain desired content in a legal marketplace than in an environment of piracy, Green said.

There's an urgent need for "a balanced approach to policy" to technological advances, but also a genuine interest in protecting copyrights, Center for Democracy and Technology Senior Policy Counsel David Sohn said. The law treats a "large pool of small-scale infringers" as it would a massive piracy ring, Sohn said. A "single set of rules for individuals and large syndicates makes no sense," he said, urging that the law let technology evolve. Sohn voiced special concern about constant invocation of piracy to justify more numerous and harsher copyright laws and increased penalties. "It is impossible to... eliminate piracy," he said. "Stop using it to justify more law." Instead, give consumers "easy, legal options," he added.

Sohn questioning the cost and effectiveness of ISP-level filtering, terming UCG site-level filtering "okay," but highlighting the risks of overly broad content blocking. Citing Jon Stewart's deft use of clips created by others to make legitimate comedic and political points, Sohn said he fears that too fine a filter will keep ordinary folk from doing the same. ISP filtering also involves deep packet inspection technology with key privacy implications, Sohn said, though UGC sites legitimately can and should filter out infringing content, within reason.

Today's laws and enforcement modes don't work, Sohn said. Most troubling to Sohn is the looming Anti-Counterfeiting Trade Agreement, being negotiated with other nations in secret by the U.S. Trade Representative. Although little is known about ACTA, what is known is especially troubling in that while it is ostensibly meant to fight counterfeit goods, it attempts to police copyright through the back door of customs enforcement, Sohn said. -- Andrew Feinberg

72 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 23, 2008 Monday

LENGTH: 640 words**HEADLINE:** Growing ID Theft Threat Requires International Approach, Prosecutor Says**BODY:**

Most incidents of identity theft are probably underreported and the true costs underestimated, said Chris Painter, principal deputy chief of the DoJ's Computer Crime and Intellectual Property Section. Speaking at the American Bar Association's CyberLaw conference, he said the rise of pervasive Internet usage has given rise to a new kind of hacker and identity thief. Painter said previous criminals acted out of a desire to prove their skills "because they could," but the fact that people now use the Internet for all sorts of commerce and banking has created a new kind of hacker with a financial motive as the primary incentive.

Today's hackers operate in far more sophisticated networks, almost always traversing international boundaries, Painter said. The networks are analogous to "real-life" criminal syndicates, he said. The organizations have a "different kind of threat profile," and often control so-called "botnets" which can comprise millions of machines that have malicious code installed on them, which Painter said can be used to capture all kinds of personal data.

Painter suggested implementing preventative measures, such as encryption to protect data. In the event those measures are unsuccessful, victims should be given assistance in fixing their records, he said, and law enforcement should be given more appropriate tools to track and combat identity theft.

The growing threat can only be countered by more cooperation among national governments, and between government and industry, said Andy Purdy, a former director of the U.S. Department of Homeland Security's National Cyber Security Division. Businesses and governments should make more frequent use of encryption whenever possible, and there should be a "more honest" discussion of the true scope of how data breaches affect identify theft, he said.

Large losses of data are generally not the root causes of identify theft, Purdy said. Instead, carelessness on the part of institutions and individuals is the factor behind most identity theft incidents, he said. Most times if money is lost, banks will often refund it rather than report a breach, he said.

Giving safe harbor to institutions that use encryption would encourage its use as well as nullify the risk of large data breaches causing massive identify theft, Purdy said. In addition, he suggested that victims of identity theft be allowed to seek restitution from institutions or defendants for the time and effort spent to fix stolen identities. Noting that as of May 2008 there were 43 state statutes dealing with identify theft and data breaches, he said the federal government should adopt legislation based on the recommendations of the Identity Theft Task Force and pre-empt the patchwork of state laws which often discourage reporting and cooperation among stakeholders. -- Andrew Feinberg

ABA CyberLaw Notebook...

Data mining should not be "a four letter word," DHS Chief Privacy Officer Hugo Teufel said Friday at the conference. While acknowledging the concerns of Congress and the public, he insisted that data mining is being used

throughout DHS in many useful ways. Teufel also called for greater harmonization of privacy protections between the U.S. and Europe. However, when questioned by Washington Internet Daily, Teufel would not back away from his Tuesday testimony before the Senate Homeland Security Committee, in which he said his office objected to the use of the word "adequacy" in a GAO report to describe the sufficiency of protections. Teufel told us that the way the European Data Protection Authority uses the word is a "term of art" and suggested that transatlantic negotiators should agree to use a different term. He also said his office would hold a two-day workshop on best practices for data mining July 24-25, having signed the Federal Register notice Friday morning. - AGF

73 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 19, 2008 Thursday

LENGTH: 887 words**HEADLINE:** Privacy Laws Need Update, Witnesses Tell Senators**BODY:**

The 1974 Privacy Act is a reliable vehicle in need of an upgrade, witnesses and senators agreed at a Wednesday hearing of the Homeland Security and Government Affairs Committee. Calling the law a "foundation for respecting individual privacy within the federal government," Chairman Joseph Lieberman, I-Conn., praised the Watergate-era mandate while calling emphatically called for its overhaul.

Lieberman's concerns result from advances in technology beyond what was imaginable in 1974, he said. "It is easier than ever for government and private entities to acquire large amounts of personal data about people -- information that can cause harm to those people if it is improperly used or disclosed," he said. Acknowledging the need for information gathering for national security purposes and law enforcement, Lieberman stressed the need to "tread carefully" and "properly balance" policy goals against privacy needs.

Lieberman was echoed by Ranking Member Susan Collins, R- Maine and Sen. Daniel Akaka, D-Hawaii. Collins seconded Lieberman's remarks on national security while calling privacy protection "a fight worth fighting in the digital age," even as people willingly share more information on blogs and social networking sites. As Lieberman did, Collins praised the 1974 Act, but urged an update committing the federal government to openness, accuracy, transparency and accountability in dealing with personal data. Akaka agreed, citing an infamous 2006 episode in which a massive database of personal information on veterans was lost when a Veterans Administration-owned laptop was stolen. Drawing on data from GAO reports commissioned after the VA incidents, Akaka said that not scrutinizing the 1974 Act for gaps risks "inaccurate information guiding our national security debates as well as Americans' access to government services and benefits."

The law not only needs a serious tune-up, but so do the tools that privacy-minded federal officials use, witnesses said. Ari Schwartz, Center for Democracy and Technology vice president, said that existing policies offer valuable tools to officials "who care about privacy," but do not "prevent indifference or wanton neglect of personal information."

Outdated Definitions, Insufficient Protections

The Internet has upended the very definitions used by government to protect personal data, Schwartz said. He cited the 1974 Act's concept of a "system of records," a phrase that excludes many modern databases and data mining methods. The 1974 Act covers records "retrieved by the name... or by some identifying symbol or other identifying particular assigned to the individual," but today's systems collect data in "clouds," scanning not just for unique identifiers but patterns. This, Schwartz said, is a glaring loophole which must be closed.

The rise of data mining companies is another loophole, Schwartz warned. The 1974 Act made it "very clear that an agency could not get around the Act by having a contractor hold the data," but that language does not apply to enormous

stores of private information collected by private companies to which the government can subscribe or purchase instead of collecting it firsthand.

A third loophole is the "routine use" exemption which overrides the 1974 Act's limits on information-sharing among agencies, Schwartz said. These waivers are "routine" even though they were meant to see use in "limited circumstances to relieve administrative burdens," he said. Schwartz noted that he counts at least 16 "routine uses" published with every Privacy Act notice. "Clearly, this is not what Congress intended," he said.

Biometric identification poses notable concerns ignored in the rush to update security procedures after 9/11, said Center for American Progress senior fellow and Ohio State University law professor Peter Swire. Of particular concern is the lack of a requirement that biometric data be encrypted and protected, he said. Swire noted that biometrics meet the "personally identifiable information" standard required by the Privacy Act, and that they require special protection because of what has been called the "biometric dilemma," in which the more you use identification, the harder it is to protect. If the government is to rely on fingerprints and other data, extra care is needed to keep those data secret, he said. Contrary to popular belief, security experts have been able to duplicate fingerprints and fool most security systems, he added. This poses a special danger, he said: "It is hard enough to get a new Social Security number once you have been the victim of identity theft. Once your fingerprint is known, though, you can't get a new finger."

Someone must be in charge of privacy at the top, senators and witnesses agreed. Akaka noted that a GAO report released today says that officials responsible for privacy at federal agencies often lack full oversight or authority to do their jobs. Noting a Homeland Security Act mandate that the DHS have a chief privacy officer, Lieberman pointed to the EU as an example of elevating privacy policy to "the highest levels of government." He suggested that the Office of Management and Budget assert more leadership on privacy, and that the executive branch may need a cabinet-level position to oversee privacy protection across government. -- Andrew Feinberg

75 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

June 18, 2008 Wednesday

LENGTH: 580 words**HEADLINE:** Cooperation Key to Piracy Fight, Committee Leaders Say**BODY:**

America must protect its intellectual property to remain the world's economic leader, Senate Judiciary Committee Chairman Patrick Leahy, D-Vt. said Tuesday at a hearing by his panel. The hearing focused on the need for more inter-agency and international cooperation in law enforcement to keep fake technology products from overwhelming the world market.

The U.S. has lagged at IP enforcement, Antitrust Subcommittee Ranking Member Orrin Hatch, R-Utah, said. He blamed an environment in which "the IP rights of others are treated causally or without any regard," due as much to inadequate enforcement as ignorance. "Some believe that if it is on the Internet, it must be free," he said. Hatch was echoed by Sen. Ben Cardin, D-Md. Cardin singled out software piracy. "We need to do a better job in our enforcement," he said.

Hatch urged an "integrated approach" to IP enforcement that weaves together state, federal and national governments. Hatch is working on legislation in the Finance Committee to address the problem, but is "not prepared to discuss the particulars" of any bill, he said. Implementing a system such as he described would take extra time, he conceded, rejecting inaction as an alternative. "As technology advances and becomes more sophisticated, so does the enemy," he said.

Counterfeiters frequently target consumer electronics, weakening consumer safety worldwide, said Brian Monks, Underwriters Laboratories vice president for anti-counterfeiting. Nearly two-thirds of counterfeit CE goods are bought at legitimate outlets, Monks said, stressing harm to consumers caused by fakes. Made with no effort at quality control, bogus devices are more prone to failure, causing injury and property damage.

The Internet is a major conduit for bogus or expired "gray-market" medicines and medical devices, said Mike Rose, Johnson & Johnson vice president for supply chain technologies. He and Monks called for more inter-agency cooperation against fakery online.

More federal leadership is needed, said Loren Yager, GAO director of international affairs. The U.S. has many legal weapons that it could use to combat counterfeiting and piracy problems, but "the current coordinating structure... lacks clear leadership," Yager said. Those gaps could be filled by giving the Homeland Security and Justice departments more money, particularly to train personnel to spot fakes, Gates Corp. Patent Counsel Jeff Thurneau said. And the U.S. should beef up the number of international trade officers at the Department of Commerce and the U.S. Trade Representative to "better equip these agencies for battle," he said.

Tuesday's hearing may be the opening Senatorial salvo in a potential pitched battle over copyright. The measure to which Hatch alluded, according to some sources, may be a companion bill to the PRO-IP Act by Rep. Howard Berman,

D- Calif. That bill passed the House by a wide margin earlier this year. NBC Universal General Counsel Rick Cotton called the hearing "a big step of starting the process of introducing a companion to PRO-IP in the Senate," while U.S. Chamber of Commerce Vice President Caroline Joiner said it "marks another important step as we look towards a Senate vote and ultimately having a strong IP bill signed into law this year." Joiner called a comprehensive IP bill "essential" and called for Congress to "solidify the government's permanent focus on intellectual property and dedicate the resources required to protect it." -- Andrew Feinberg

76 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
CONSUMER ELECTRONICS DAILY

June 18, 2008 Wednesday

LENGTH: 580 words**HEADLINE:** Cooperation Key to Piracy Fight, Committee Leaders Say**BODY:**

America must protect its intellectual property to remain the world's economic leader, Senate Judiciary Committee Chairman Patrick Leahy, D-Vt. said Tuesday at a hearing by his panel. The hearing focused on the need for more inter-agency and international cooperation in law enforcement to keep fake technology products from overwhelming the world market.

The U.S. has lagged at IP enforcement, Antitrust Subcommittee Ranking Member Orrin Hatch, R-Utah, said. He blamed an environment in which "the IP rights of others are treated causally or without any regard," due as much to inadequate enforcement as ignorance. "Some believe that if it is on the Internet, it must be free," he said. Hatch was echoed by Sen. Ben Cardin, D-Md. Cardin singled out software piracy. "We need to do a better job in our enforcement," he said.

Hatch urged an "integrated approach" to IP enforcement that weaves together state, federal and national governments. Hatch is working on legislation in the Finance Committee to address the problem, but is "not prepared to discuss the particulars" of any bill, he said. Implementing a system such as he described would take extra time, he conceded, rejecting inaction as an alternative. "As technology advances and becomes more sophisticated, so does the enemy," he said.

Counterfeiters frequently target consumer electronics, weakening consumer safety worldwide, said Brian Monks, Underwriters Laboratories vice president for anti-counterfeiting. Nearly two-thirds of counterfeit CE goods are bought at legitimate outlets, Monks said, stressing harm to consumers caused by fakes. Made with no effort at quality control, bogus devices are more prone to failure, causing injury and property damage.

The Internet is a major conduit for bogus or expired "gray-market" medicines and medical devices, said Mike Rose, Johnson & Johnson vice president for supply chain technologies. He and Monks called for more inter-agency cooperation against fakery online.

More federal leadership is needed, said Loren Yager, GAO director of international affairs. The U.S. has many legal weapons that it could use to combat counterfeiting and piracy problems, but "the current coordinating structure... lacks clear leadership," Yager said. Those gaps could be filled by giving the Homeland Security and Justice departments more money, particularly to train personnel to spot fakes, Gates Corp. Patent Counsel Jeff Thurneau said. And the U.S. should beef up the number of international trade officers at the Department of Commerce and the U.S. Trade Representative to "better equip these agencies for battle," he said.

Tuesday's hearing may be the opening Senatorial salvo in a potential pitched battle over copyright. The measure to which Hatch alluded, according to some sources, may be a companion bill to the PRO-IP Act by Rep. Howard Berman,

D- Calif. That bill passed the House by a wide margin earlier this year. NBC Universal General Counsel Rick Cotton called the hearing "a big step of starting the process of introducing a companion to PRO-IP in the Senate," while U.S. Chamber of Commerce Vice President Caroline Joiner said it "marks another important step as we look towards a Senate vote and ultimately having a strong IP bill signed into law this year." Joiner called a comprehensive IP bill "essential" and called for Congress to "solidify the government's permanent focus on intellectual property and dedicate the resources required to protect it." - Andrew Feinberg

77 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 18, 2008 Wednesday

LENGTH: 584 words**HEADLINE:** Cooperation Key to Piracy Fight, Committee Leaders Say**BODY:**

America must protect its intellectual property to remain the world's economic leader, Senate Judiciary Committee Chairman Patrick Leahy, D-Vt. said Tuesday at a hearing by his panel. The hearing focused on the need for more inter-agency and international cooperation in law enforcement to keep fake technology products from overwhelming the world market.

The U.S. has lagged at IP enforcement, Antitrust Subcommittee Ranking Member Orrin Hatch, R-Utah, said. He blamed an environment in which "the IP rights of others are treated causally or without any regard," due as much to inadequate enforcement as ignorance. "Some believe that if it is on the Internet, it must be free," he said. Hatch was echoed by Sen. Ben Cardin, D-Md. Cardin singled out software piracy. "We need to do a better job in our enforcement," he said.

Hatch urged an "integrated approach" to IP enforcement that weaves together state, federal and national governments. Hatch is working on legislation in the Finance Committee to address the problem, but is "not prepared to discuss the particulars" of any bill, he said. Implementing a system such as he described would take extra time, he conceded, rejecting inaction as an alternative. "As technology advances and becomes more sophisticated, so does the enemy," he said.

Counterfeiters frequently target consumer electronics, weakening consumer safety worldwide, said Brian Monks, Underwriters Laboratories vice president for anti-counterfeiting. Nearly two-thirds of counterfeit CE goods are bought at legitimate outlets, Monks said, stressing harm to consumers caused by fakes. Made with no effort at quality control, bogus devices are more prone to failure, causing injury and property damage.

The Internet is a major conduit for bogus or expired "gray-market" medicines and medical devices, said Mike Rose, Johnson & Johnson vice president for supply chain technologies. He and Monks called for more inter-agency cooperation against fakery online.

More federal leadership is needed, said Loren Yager, GAO director of international affairs. The U.S. has many legal weapons that it could use to combat counterfeiting and piracy problems, but "the current coordinating structure... lacks clear leadership," Yager said. Those gaps could be filled by giving the Homeland Security and Justice departments more money, particularly to train personnel to spot fakes, Gates Corp. Patent Counsel Jeff Thurneau said. And the U.S. should beef up the number of international trade officers at the Department of Commerce and the U.S. Trade Representative to "better equip these agencies for battle," he said.

Tuesday's hearing may be the opening senatorial salvo in a potential pitched battle over copyright. The measure to which Hatch alluded, according to some sources, may be a companion bill to the PRO-IP Act by House IP

Subcommittee Chairman Howard Berman, D-Calif. That bill passed the House by a wide margin earlier this year. NBC Universal General Counsel Rick Cotton called the hearing "a big step of starting the process of introducing a companion to PRO-IP in the Senate," while U.S. Chamber of Commerce Vice President Caroline Joiner said it "marks another important step as we look towards a Senate vote and ultimately having a strong IP bill signed into law this year." Joiner called a comprehensive IP bill "essential" and called for Congress to "solidify the government's permanent focus on intellectual property and dedicate the resources required to protect it." -- Andrew Feinberg

79 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 17, 2008 Tuesday

LENGTH: 956 words**HEADLINE:** Voluntary Nature of ISP Agreements with AG Questioned**BODY:**

A trend of "voluntary" agreements between corporations and law enforcement raises serious constitutional questions, attorneys and privacy advocates say. The latest example was last week's announcement of an agreement between the New York Attorney General's office and Verizon, Time Warner Cable and Sprint (WID June 12 p4). The ISPs agreed either to block or remove entirely access to Usenet discussion boards known to carry child pornography, and to block access to offending sites as they are identified by the National Center for Missing and Exploited Children.

Other recent instances include pacts between Facebook, MySpace and 49 state attorneys general leading to creation of the Internet Safety Task Force, which has expanded to include many different Internet companies. As the New York agreement does, the Facebook and MySpace arrangements followed intense law enforcement pressure on the sites to crack down on alleged predation against children. Among the AGs cited as leaning hardest on the sites was North Carolina's Roy Cooper. He, as many colleagues elsewhere, threatened the social networking sites with such cudgels as imposition of myriad age verification requirements that would have made it difficult to register new users. MySpace entered into a collective agreement with the AGs in January. Facebook followed suit last month. The agreements are completely voluntary, say all the parties involved.

The meaning of "voluntary" is a different matter, the Progress and Freedom Foundation's Adam Thierer said: "Voluntary agreements between industry and law enforcement officials or government have always raised questions" as to their enforceability and constitutionality, he said. Such arrangements comprise "an ambiguous legal issue," he said, noting that none has undergone the test of court challenge.

The agreements may be unconstitutional if coerced, said John Morris, Chief Counsel for the Center for Democracy & Technology. Morris, lead attorney on the landmark *Reno v. ACLU* case, has specific concerns about the decision by Verizon and Sprint to stop carrying only the alt.* hierarchy of groups. That hierarchy includes thousands of discussion groups whose topics range from motorcycle maintenance to Late Night with David Letterman. The ISPs left other hierarchies untouched. Such selective blocking of content would be unconstitutional if done by law, but the agreement's voluntary nature leaves the question of who would have standing to challenge it unclear, Morris said. This unique standing issue puts the agreements in uncharted territory, Thierer said. Both sides may stress the deals' voluntary nature, but they may not be legally enforceable, he said.

The agreement's true "enforcement" lies in the implied threat of regulation "above and beyond" what the agreements stipulate, Thierer said. That threat is a mandate that the sites engage in age verification, which he called the "sword of Damocles" over social networking services' necks. And an age verification scheme raises even tougher questions, since it would involve minors entering personal data to be checked against a database, he said. Such records would be especially useful to identity thieves, since most children have clean credit records, Thierer said.

The constitutional test lies in the agreements' context, Morris said. "Are they agreements that these providers voluntarily entered into?" he asked. In the New York case, he suggested, if the pacts result from "government coercion," they're most likely unconstitutional. "The government cannot require ISPs to block access to newsgroups that carry lawful content." A 2004 Philadelphia U.S. District Court decision voided a Pennsylvania law requiring ISPs to "remove or disable access to child pornography items 'residing on or accessible through its service' after notification by the Pennsylvania Attorney General."

The agreements may be better than the alternative of government regulation, Thierer said. "I know these AG's, for example, have been very hungry to go much, much further, and impose some comprehensive regulatory scheme on the entire Internet," he said. "It's sort of a lesser of two evils question, right?" Some of the provisions, he said, are "quite laudable" in their ultimate goal of protecting children.

Some might call the agreements a form of regulatory or economic "blackmail," Morris and Thierer agreed. In effect the states have declared that "if you don't agree with what we want you to agree to, we're going to criticize you in the marketplace," Morris said. Not judging the constitutional arguments, Morris acknowledged the power of the AGs' bully pulpit: "It is effective with mass-market companies."

The trend toward "voluntary" agreements isn't new, said former FCC Commissioner Harold Furchtgott-Roth. He recalled many instances in which the commission pressured companies into "voluntary" actions before the commission would grant a license transfer or approve a merger. The specifics obviously differ, but the concern is similar -- a situation in which a governmental agency "with a wide range of enormous powers" exerts pressure on a company to achieve a regulatory goal, he said. That is an acceptable goal when attempting to bring a company into compliance with an existing law or regulation, but the New York AG scenario "sounds pretty awful," Furchtgott-Roth said. He contrasted it with similar situations during his tenure at the FCC, "a regulatory agency which has to provide some kind of privilege" in exchange for obtaining adherence to a condition. Crossing the FCC might not grab national headlines, but crossing a state AG and being dragged into the headlines is a "game of chicken" many businesses would rather avoid, he said. - Andrew Feinberg

81 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

June 16, 2008 Monday

LENGTH: 421 words**HEADLINE:** FTC Commissioner Rosch: Antitrust No Net Neutrality Panacea**BODY:**

Antitrust and consumer protection laws have places in the net neutrality debate, FTC Commissioner Thomas Rosch said in a keynote at Friday's Broadband Summit. The shift in concern over the possibility of "quid pro quo" deals for preferred content delivery to network management raises consumer protection issues, but none so complex that current law can't address them, Rosch said.

The main question is whether "providers should be able to totally control their networks," Rosch said. He cited network operators' claims that neutrality mandates could destabilize infrastructure at risk. Consumer protection concerns arise from the users' point of view of network traffic as a "black box," he said, adding that without transparent network management, "suspicion is inevitable."

That suspicion can be assuaged by "clearly and conspicuously" disclosing practices and policies, Rosch said. Consumers are best served when they can compare similar services among providers, he added. That comes only through "clear and conspicuous disclosure of material terms," he said. Precedent bars deceptive or unfair practices by information services, he said, citing cases involving AOL, CompuServe and Prodigy.

Antitrust enforcement can solve few, "if any problems" in the area of net neutrality, Rosch said, invoking his work as an antitrust litigator. With few exceptions, the Sherman and Clayton Acts have "limited application" to net neutrality, he noted. However, he said, citing the Madison River case (CD March 4/05 p12), consensus on that decision "surprised me as an antitrust lawyer." A broadband provider's "refusal to deal" in an adjacent market, like phone service, would be difficult to litigate under Section 2 of the Sherman Act, said Rosch. A Section 2 proceeding would be even less appropriate for the Comcast-BitTorrent matter, he said. Under Section 2, BitTorrent's only reasonable claim would be that Comcast caused a "loss of consumer confidence" in BitTorrent's competing video delivery service, he added.

Other recent net neutrality issues fall outside antitrust law, Rosch said. The Verizon-NARAL episode involves content, while antitrust law focuses on "economic effects and price competition," he said.

The FTC hopes to examine net neutrality in relation to Section 5 of the FTC Act, Rosch said. He hesitates to "over-promise" on antitrust law's effectiveness in that area, he said. Invoking the law of unintended consequences, he cautioned against haste in seeking specific net neutrality legislation. - Andrew Feinberg

82 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 16, 2008 Monday

LENGTH: 1075 words**HEADLINE:** Google-Yahoo Teed Up at Senate Antitrust, House Consumer Protection Subcommittees**BODY:**

Antitrust is on everyone's minds when it comes to the Google-Yahoo deal for search and contextual advertising, announced late Thursday after Yahoo said it had thrown in the towel with Microsoft (WID June 13 p6). Several analysts said the deal would get strong scrutiny from the Justice Department. Gauging from early Hill reaction, multiple hearings seem likely, though not immediately at a key committee examining online advertising. The conditions of the arrangement are flexible enough to give Google and Yahoo a way out, due to underperformance or ownership changes.

The deal between "direct competitors" could have "far-reaching" consequences for advertisers and consumers, said Senate Antitrust Subcommittee Chairman Herb Kohl, D-Wis. "We plan to investigate the competitive and privacy implications of this deal further" in subcommittee, he said. The House Consumer Protection Subcommittee, which promised a hearing following Microsoft's intended courtship of Yahoo (WID Feb 6 p1), is "preparing to hold a hearing on this important issue this summer," said Chairman Bobby Rush, D-Ill. Ranking Member Ed Whitfield, R-Ky., said he was concerned about how consumers' "data sets may be combined for future use." The subcommittee's planned spring hearing on online advertising never materialized, though.

The Senate Commerce Committee probably won't focus on the deal at its Wednesday hearing on privacy in online advertising (WID June 13 p4), though the witness list won't be finalized until Monday, an aide told us. There's also no immediate plan for a standalone hearing, though that could change, the aide said. The FTC probably won't get involved because DoJ has claimed jurisdiction, Commissioner Thomas Rosch told us Friday at the Broadband Policy Summit in Washington. (See separate report in this issue.) Rosch said he was "very reluctant" to comment on what effect the deal could have in terms of access to some consumers' information.

Google took pains to emphasize why it thinks the deal would pass muster with regulators. Google provides "similar services" to Ask.com and AOL, said Omid Kordestani, senior vice president of global sales and business development, on the official Google blog. "This is not a merger," but rather gives Yahoo access to Google's advertising technology, he said, comparing the "commonplace" arrangement to that between Canon and HP for laser printer engines. Yahoo will remain a competitor and have "continued incentive to keep improving and innovating," Kordestani said: "Yahoo can use our technology as much or as little as it chooses," and make similar deals with others.

Perhaps most importantly for regulators, Google's share of search traffic won't rise and the company won't raise ad prices, since they're determined by auction, Kordestani said. The deal has a 4-year initial term and can be renewed twice under 3-year terms at Yahoo's option, though the companies said they'll voluntarily delay implementation up to three and a half months for Justice Department review. Google and Yahoo also said they'll work on interoperability between their instant-messaging services.

The deal gets complicated when it comes to revenue benchmarks and potential changes of ownership, according to

a Yahoo 8-K filing. Google can break the deal after 10 months, and each month thereafter, if revenue doesn't hit roughly \$83 million for the four prior calendar months. Yahoo will owe Google \$250 million if the arrangement is scrapped in the first two years because of a "change in control," defined as half of Yahoo's shares being purchased by another party, or 35 percent being purchased by Microsoft, Time Warner or News Corp. The so-called kill fee wouldn't apply for a change of control "triggered by" Microsoft's acquisition of more than 15 percent of outstanding shares or more than 5 percent of shares directly from Yahoo, or if Microsoft buys any part of Yahoo representing more than 1 percent of its annual revenue.

Are Google and Yahoo 'Substitutes'?

The nod to DoJ review "suggests that DoJ believes the arrangement poses serious issues," said Stifel Nicolaus analysts. The deal's application to U.S. and Canada alone seems intended to avoid antitrust scrutiny from the European Union, where Google had a tougher time getting through the DoubleClick merger, they said. To pass muster with DoJ, the companies must explain "why the efficiencies of the deal won't ultimately lead advertisers to move to Google, leaving Yahoo without a viable search advertising product and Google as the only search advertising game in town," they said.

The use of auctions to allocate ads backs up the "inherent caution" of DoJ Antitrust Chief Thomas Barnett over challenging outsourcing transactions, Stanford Group analyst Paul Gallant said. But if a broad array of advertisers tell DoJ they consider the companies "reasonable substitutes," the agency will be skeptical of the deal, he said. Yahoo must show DoJ that it has a "financial incentive" to continue competing in portions of search where it's even with Google, Gallant said.

"The truth is that this will cause even more advertisers to flee Yahoo's platform," said TechCrunch founder Michael Arrington. "Which will drive auction-determined ad rates down. Which will drive Yahoo to take more Google ads... It's a vicious cycle and they will have no choice, as a public company, but to rely more and more on Google as time goes on," he said. It would be better for Yahoo's share price for its Panama ad operation to be fully outsourced, said American Technology Research analyst Rob Sanderson. The firm estimates that would bring in \$700 million, instead of Yahoo's estimated \$250 million to \$450 million from the Google deal in the first year, he said.

DoJ "should now realize that it's dealing with what is essentially a monopoly," said Steve Pociask, president of the free-market American Consumer Institute. "When all would-be advertisers are forced to participate in the same auction, prices will skyrocket and smaller players can be more easily shut out," said Harry Alford, president of the National Black Chamber of Commerce. But Google and Yahoo got some love from the Computer and Communications Industry Association. President Ed Black said there would be "no diminution of Yahoo's competitive ability" and thus no harm to consumers. Yahoo will remain an "independent platform for innovation," which "has some advantages," Black said. --
Greg Piper, Andrew Feinberg

84 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 16, 2008 Monday

LENGTH: 452 words**HEADLINE:** Broadband Summit Panel Sees Positive Steps on Net Neutrality**BODY:**

The debate on net neutrality has evolved from an academic concern into concrete issues, panelists said at Friday's Broadband Summit. Daniel Brenner, NCTA senior vice president, said "the debate has intensified" since last year's summit and is still a significant part of his organization's agenda. Free Press Policy Director Ben Scott said both public awareness and regulatory scrutiny had increased, but former Clinton press secretary and Public Strategies partner Mike McCurry said the only thing that has changed is that the network carries more data. McCurry, who has lobbied on behalf of anti-neutrality groups, said a "vigilant FCC" would preclude the need for new regulation or legislation. CTIA Vice President Christopher Guttman-McCabe said network neutrality legislation would provide a "disincentive to invest" in new capacity.

Reaction to recent events has led to change, said Public Knowledge President Gigi Sohn, citing the FCC's field hearings in Cambridge, Mass., and Palo Alto, Calif., as "huge" developments in the debate as the FCC has sought to define what constitutes "reasonable network management." She disagreed with FTC Commissioner Thomas Rosch's use of the word "managing" to describe Comcast's actions that led to the hearings, insisting that Comcast had blocked BitTorrent traffic, not managed it. Brian Bieron, eBay senior director of government affairs, agreed, calling it a "concrete example of discriminatory treatment."

In answer to a question on what network management is reasonable, Bieron replied with several questions: "First, does the management protect non-network based services from competitors? Second - do users know?" He suggested that non-discriminatory measures like bandwidth caps on high- volume use would be considered reasonable.

Sohn said: "I don't want network providers looking at my data and making value judgements - who has control?" Users should be able to choose their own priorities, she said, saying even something like an E911 call should be her choice to prioritize or not.

Sohn said she was "excited" about the "open access" requirements of the recent 700 MHz auction but cautioned that all she had seen were announcements, and expressed worry that Verizon would confine some devices to MVNOs or practice some form of price discrimination. Verizon Senior Vice President Kathryn Brown said she couldn't respond, saying the open access plans were in the development stages, and it was something that Verizon was "working hard on."

Brenner said the openness rules still required a "regulatory humility" in enforcement. Scott compared them to inter-LATA and program access rules, which he said had been widely successful over the long term. - Andrew Feinberg

85 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 16, 2008 Monday

LENGTH: 1075 words**HEADLINE:** Google-Yahoo Teed Up at Senate Antitrust, House Consumer Protection Subcommittees**BODY:**

Antitrust is on everyone's minds when it comes to the Google-Yahoo deal for search and contextual advertising, announced late Thursday after Yahoo said it had thrown in the towel with Microsoft (WID June 13 p6). Several analysts said the deal would get strong scrutiny from the Justice Department. Gauging from early Hill reaction, multiple hearings seem likely, though not immediately at a key committee examining online advertising. The conditions of the arrangement are flexible enough to give Google and Yahoo a way out, due to underperformance or ownership changes.

The deal between "direct competitors" could have "far-reaching" consequences for advertisers and consumers, said Senate Antitrust Subcommittee Chairman Herb Kohl, D-Wis. "We plan to investigate the competitive and privacy implications of this deal further" in subcommittee, he said. The House Consumer Protection Subcommittee, which promised a hearing following Microsoft's intended courtship of Yahoo (WID Feb 6 p1), is "preparing to hold a hearing on this important issue this summer," said Chairman Bobby Rush, D-Ill. Ranking Member Ed Whitfield, R-Ky., said he was concerned about how consumers' "data sets may be combined for future use." The subcommittee's planned spring hearing on online advertising never materialized, though.

The Senate Commerce Committee probably won't focus on the deal at its Wednesday hearing on privacy in online advertising (WID June 13 p4), though the witness list won't be finalized until Monday, an aide told us. There's also no immediate plan for a standalone hearing, though that could change, the aide said. The FTC probably won't get involved because DoJ has claimed jurisdiction, Commissioner Thomas Rosch told us Friday at the Broadband Policy Summit in Washington. (See separate report in this issue.) Rosch said he was "very reluctant" to comment on what effect the deal could have in terms of access to some consumers' information.

Google took pains to emphasize why it thinks the deal would pass muster with regulators. Google provides "similar services" to Ask.com and AOL, said Omid Kordestani, senior vice president of global sales and business development, on the official Google blog. "This is not a merger," but rather gives Yahoo access to Google's advertising technology, he said, comparing the "commonplace" arrangement to that between Canon and HP for laser printer engines. Yahoo will remain a competitor and have "continued incentive to keep improving and innovating," Kordestani said: "Yahoo can use our technology as much or as little as it chooses," and make similar deals with others.

Perhaps most importantly for regulators, Google's share of search traffic won't rise and the company won't raise ad prices, since they're determined by auction, Kordestani said. The deal has a 4-year initial term and can be renewed twice under 3-year terms at Yahoo's option, though the companies said they'll voluntarily delay implementation up to three and a half months for Justice Department review. Google and Yahoo also said they'll work on interoperability between their instant-messaging services.

The deal gets complicated when it comes to revenue benchmarks and potential changes of ownership, according to

a Yahoo 8-K filing. Google can break the deal after 10 months, and each month thereafter, if revenue doesn't hit roughly \$83 million for the four prior calendar months. Yahoo will owe Google \$250 million if the arrangement is scrapped in the first two years because of a "change in control," defined as half of Yahoo's shares being purchased by another party, or 35 percent being purchased by Microsoft, Time Warner or News Corp. The so-called kill fee wouldn't apply for a change of control "triggered by" Microsoft's acquisition of more than 15 percent of outstanding shares or more than 5 percent of shares directly from Yahoo, or if Microsoft buys any part of Yahoo representing more than 1 percent of its annual revenue.

Are Google and Yahoo 'Substitutes'?

The nod to DoJ review "suggests that DoJ believes the arrangement poses serious issues," said Stifel Nicolaus analysts. The deal's application to U.S. and Canada alone seems intended to avoid antitrust scrutiny from the European Union, where Google had a tougher time getting through the DoubleClick merger, they said. To pass muster with DoJ, the companies must explain "why the efficiencies of the deal won't ultimately lead advertisers to move to Google, leaving Yahoo without a viable search advertising product and Google as the only search advertising game in town," they said.

The use of auctions to allocate ads backs up the "inherent caution" of DoJ Antitrust Chief Thomas Barnett over challenging outsourcing transactions, Stanford Group analyst Paul Gallant said. But if a broad array of advertisers tell DoJ they consider the companies "reasonable substitutes," the agency will be skeptical of the deal, he said. Yahoo must show DoJ that it has a "financial incentive" to continue competing in portions of search where it's even with Google, Gallant said.

"The truth is that this will cause even more advertisers to flee Yahoo's platform," said TechCrunch founder Michael Arrington. "Which will drive auction-determined ad rates down. Which will drive Yahoo to take more Google ads... It's a vicious cycle and they will have no choice, as a public company, but to rely more and more on Google as time goes on," he said. It would be better for Yahoo's share price for its Panama ad operation to be fully outsourced, said American Technology Research analyst Rob Sanderson. The firm estimates that would bring in \$700 million, instead of Yahoo's estimated \$250 million to \$450 million from the Google deal in the first year, he said.

DoJ "should now realize that it's dealing with what is essentially a monopoly," said Steve Pociask, president of the free-market American Consumer Institute. "When all would-be advertisers are forced to participate in the same auction, prices will skyrocket and smaller players can be more easily shut out," said Harry Alford, president of the National Black Chamber of Commerce. But Google and Yahoo got some love from the Computer and Communications Industry Association. President Ed Black said there would be "no diminution of Yahoo's competitive ability" and thus no harm to consumers. Yahoo will remain an "independent platform for innovation," which "has some advantages," Black said. --
Greg Piper, Andrew Feinberg

87 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 16, 2008 Monday

LENGTH: 452 words**HEADLINE:** Broadband Summit Panel Sees Positive Steps on Net Neutrality**BODY:**

The debate on net neutrality has evolved from an academic concern into concrete issues, panelists said at Friday's Broadband Summit. Daniel Brenner, NCTA senior vice president, said "the debate has intensified" since last year's summit and is still a significant part of his organization's agenda. Free Press Policy Director Ben Scott said both public awareness and regulatory scrutiny had increased, but former Clinton press secretary and Public Strategies partner Mike McCurry said the only thing that has changed is that the network carries more data. McCurry, who has lobbied on behalf of anti-neutrality groups, said a "vigilant FCC" would preclude the need for new regulation or legislation. CTIA Vice President Christopher Guttman-McCabe said network neutrality legislation would provide a "disincentive to invest" in new capacity.

Reaction to recent events has led to change, said Public Knowledge President Gigi Sohn, citing the FCC's field hearings in Cambridge, Mass., and Palo Alto, Calif., as "huge" developments in the debate as the FCC has sought to define what constitutes "reasonable network management." She disagreed with FTC Commissioner Thomas Rosch's use of the word "managing" to describe Comcast's actions that led to the hearings, insisting that Comcast had blocked BitTorrent traffic, not managed it. Brian Bieron, eBay senior director of government affairs, agreed, calling it a "concrete example of discriminatory treatment."

In answer to a question on what network management is reasonable, Bieron replied with several questions: "First, does the management protect non-network based services from competitors? Second - do users know?" He suggested that non-discriminatory measures like bandwidth caps on high- volume use would be considered reasonable.

Sohn said: "I don't want network providers looking at my data and making value judgements - who has control?" Users should be able to choose their own priorities, she said, saying even something like an E911 call should be her choice to prioritize or not.

Sohn said she was "excited" about the "open access" requirements of the recent 700 MHz auction but cautioned that all she had seen were announcements, and expressed worry that Verizon would confine some devices to MVNOs or practice some form of price discrimination. Verizon Senior Vice President Kathryn Brown said she couldn't respond, saying the open access plans were in the development stages, and it was something that Verizon was "working hard on."

Brenner said the openness rules still required a "regulatory humility" in enforcement. Scott compared them to inter-LATA and program access rules, which he said had been widely successful over the long term. - Andrew Feinberg

89 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 12, 2008 Thursday

LENGTH: 617 words**HEADLINE:** Senators Want Better Anti-Spyware Tools; FTC Says Civil Penalties Needed**BODY:**

Existing legislation hasn't stemmed the spread of spyware and requires more teeth, said witnesses at a Senate Commerce Committee hearing Wednesday on the Counter Spy Act (S-1625). While a few witnesses expressed concerns about unintended consequences, and the FTC said it believes existing tools are effective but could use civil penalties, most witnesses and senators said new more action is needed to protect consumers from unwanted spyware, malware and adware.

Spyware is "a pervasive problem that demands swift action," said Sen. Mark Pryor, D-Ark., who chaired the hearing and has co-sponsored anti-spyware legislation. Citing a Consumer Reports study that one in 11 consumers have infected computers, and pay on average \$100 to fix the problem, Sen. Bill Nelson, D-Fla., agreed, and expressed a desire to give the FTC the authority to go after spyware vendors.

Stopping spyware is a priority and existing tools are effective, said Eileen Harrington, deputy director of the FTC's Consumer Protection Bureau. Citing 11 enforcement actions against vendors that the commission has taken since 2001, she said the effort to reduce adware has been effective, and pointed to a joint consumer education effort.

Legislation should be technology-neutral and not be obsoleted easily, said Sen. David Vitter, R-La., who added that criminals are not likely to obey anti-spyware laws. However, Nelson was skeptical that requiring vendors to provide a "readily identifiable means" of removal was adequate, asking Harrington for a definition, which she said was one that a "reasonable consumer" would be able to use. Referring to the FTC's recent Zango case, he asked if the FTC would review software on a case-by-case basis. She said it would continue to apply the "reasonable consumer" standard.

Nelson asked if an operating system toolbar would be sufficient. She responded that a system's add-remove function would be sufficient: "Generally, we would expect it would be apparent." Nelson was skeptical of what appeared to be complacency by the FTC, asking if such a definition would apply to keystroke loggers. Harrington replied that those pieces of software would be illegal, and couldn't tell Nelson how a consumer could remove it, saying a user's antivirus software would have to handle the task. With respect to regulatory tools, Harrington told the committee that except for the addition of civil penalties, "we have enough and are using it."

What some call spyware can "foster commerce," and self- regulation is the best solution, said Jerry Cerasale, vice president of the Direct Marketing Association. He told Pryor that DMA had supported legislation such as CAN-SPAM when there were "criminal" elements involved, but he feared unintended consequences. He said he agreed with the FTC that existing tools would be adequate and suggested chilling effects would occur if advertising software were to be included in an "overly broad" definition of spyware. Pryor repeatedly asked him and the other witnesses to define the term.

The PC is personal property, Pryor said. Vincent Weafer, Symantec vice president for security response, called spyware a "significant threat," and lauded the senators for including a provision in the legislation that would prohibit software vendors' unauthorized monitoring of users' activities. Asked later how this position jibes with BSA members, most notably Microsoft's monitoring and disabling of what it finds to be pirated software, such as in Microsoft's Windows Genuine Advantage program, he replied: "We support the goal of helping anti-spyware software vendors to protect the consumer, but we also need the ability to protect software vendors from theft." -- Andrew Feinberg

91 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

June 11, 2008 Wednesday

LENGTH: 667 words**HEADLINE:** Tate Concerned about Kids' Use of Convergence Devices, Streaming Content**BODY:**

Interactive media present a new set of risks to children, FCC Commissioners Deborah Tate and Jonathan Adelstein said at the PointSmart.ClickSafe Summit. In separate keynotes, the commissioners said the issues require attention to ensure that children remain safe in a broadband-connected world.

Saying she would rather discuss issues than statistics, Tate said the Internet is becoming a part of everyday life for kids and teens, and "what was once considered and described as a virtual world... is now our children's very real world." This expansion, Tate said, has brought to light a new set of risks that young people face in their online lives. The Internet is becoming more important to young people, she said, noting that kids now are creating their own content on video sharing and social networking site. She said the phenomenon presents even greater dangers as kids share personal information and photographs through social networks.

Cyberbullying is Tate's latest interest; it was piqued by the recent Megan Meier case. Citing statistics that one in four children have experienced some kind of cyberbullying, Tate said her strong feelings on the issue come from her experience "as a mother...and as a policymaker." Tate said cyberbullying is not only a technological issue but a health and welfare threat.

Convergence and the near-ubiquity of the Internet on mobile phones make parental and educational involvement even more important, Tate said. She also urged the cable and wireless industries to help create a safe environment for young people.

Adelstein said protecting children in the virtual world is not dissimilar from the real world, stressing parental involvement as the first line of defense. He said a major threat to children's online mental and physical health comes from TV as well as the Internet. One danger that's being overlooked on both TV and the Internet, he said, is "excessive commercialism for unhealthy products." He called parents the "first, last, and best line of defense against all forms of objectionable content" and praised industry efforts to increase online literacy. However, he said some problems by their very nature can be solved only by regulation, even if the regulations are unpopular among companies: "It's another thing entirely to take real action that can make a difference."

The commission urgently needs to take action on several open rulemakings on matters affecting children, Adelstein said, adding they have been open for more than a year and enjoy majority support. He pleaded for the public to file comments on the rulemaking on whether existing advertising rules are in line with the policy goals of the Children's Television Act. An item on embedded advertising has been under circulation for more than a year and has been held up despite majority support and being proposed by Chairman Martin himself, Adelstein said.

Convergence of TV and the Internet poses further dangers to children in the form of commercials, Adelstein said,

as interactive media begin to contain more and more advertising content. Adelstein criticized recently passed media ownership rules, saying excessive commercialization is a consequence of consolidation. He urged Martin to issue a final rule banning interactive advertising to children, and expressed hope that his colleagues would support it.

Adelstein warned that the increased use of product placement requires updated rules, and he called for a commission vote on the sponsorship identification rules. "People need to see it and read it - not just have a crawler that they need to read with a magnifying glass."

Just because interactive TV is new doesn't mean it's too soon to act, Adelstein said. Referencing a Kaiser study on online food advertising, and a recent Washington Post series on childhood obesity, he said "we know what is going to happen," saying that if the Commission doesn't act on interactive advertising to children before it becomes well established, "it could be too late." - Andrew Feinberg

92 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

June 11, 2008 Wednesday

LENGTH: 443 words**HEADLINE:** Group to Study Online Safety Practices for Kids**BODY:**

Cooperation among stakeholders is the best way to protect children in a wired world, said a panel of industry executives and child protection experts at Tuesday's PointSmart.ClickSafe summit. The communications industry faces a difficult choice on how much responsibility it should take, said the Progress and Freedom Foundation's Adam Thierer in response to a question from Comcast government affairs advisor Torie Clarke. The choice encompasses both the content it provides and what tools are offered to parents, Thierer said, and shouldn't include self-censorship. Thierer said the industry should not have to take responsibility for content.

Parents care more about the Internet than TV, said Alexandra Wilson, Cox vice president of public policy. She said the company began to ask customers about content filters after the Janet Jackson's "wardrobe malfunction" incident and was surprised to learn that TV content was not the first concern parents had with what their children view.

Online safety is an issue the entire industry can tackle, Verizon Public Affairs' executive directory for internet and technology policy Michael McKeehan agreed, saying providers around the world were working together on best practices for child protection standards: "It's very important that we have this national and international cooperation." Content providers should provide more options for kid-friendly places, Disney Vice President Susan Fox said, saying maintaining a safe environment is important to the company's business.

An industry working group on child protection will hold its first meeting Wednesday, Clarke said. The group has an abundance of source material to draw on, said Thierer, pointing to commissions in the U.K. and Australia, which placed strong emphasis on education and media literacy. While the commissions considered filtering technologies, he said, they concluded there's no substitute for education in protecting kids online.

When it comes to child safety, Thierer said, America tends to "regulate first, educate later," citing a PFF/CDT survey that found that only two of 37 bills dealing with technology or online safety before Congress last year focused on education. "This is a problem," he said, suggesting money spent on litigation could instead be spent on an educational program such as the U.S. Forest Service's Smokey the Bear campaign, and that the focus should be on making kids "responsible cyber-citizens." While some states, including Virginia, have created online education requirements, Thierer said more could be done with a nationwide effort. "I think we need that kind of program at the Federal level." -- Andrew Feinberg

94 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 11, 2008 Wednesday

LENGTH: 443 words**HEADLINE:** Group to Study Online Safety Practices for Kids**BODY:**

Cooperation among stakeholders is the best way to protect children in a wired world, said a panel of industry executives and child protection experts at Tuesday's PointSmart.ClickSafe summit. The communications industry faces a difficult choice on how much responsibility it should take, said the Progress and Freedom Foundation's Adam Thierer in response to a question from Comcast government affairs advisor Torie Clarke. The choice encompasses both the content it provides and what tools are offered to parents, Thierer said, and shouldn't include self-censorship. Thierer said the industry should not have to take responsibility for content.

Parents care more about the Internet than TV, said Alexandra Wilson, Cox vice president of public policy. She said the company began to ask customers about content filters after the Janet Jackson's "wardrobe malfunction" incident and was surprised to learn that TV content was not the first concern parents had with what their children view.

Online safety is an issue the entire industry can tackle, Verizon Public Affairs' executive directory for internet and technology policy Michael McKeehan agreed, saying providers around the world were working together on best practices for child protection standards: "It's very important that we have this national and international cooperation." Content providers should provide more options for kid-friendly places, Disney Vice President Susan Fox said, saying maintaining a safe environment is important to the company's business.

An industry working group on child protection will hold its first meeting Wednesday, Clarke said. The group has an abundance of source material to draw on, said Thierer, pointing to commissions in the U.K. and Australia, which placed strong emphasis on education and media literacy. While the commissions considered filtering technologies, he said, they concluded there's no substitute for education in protecting kids online.

When it comes to child safety, Thierer said, America tends to "regulate first, educate later," citing a PFF/CDT survey that found that only two of 37 bills dealing with technology or online safety before Congress last year focused on education. "This is a problem," he said, suggesting money spent on litigation could instead be spent on an educational program such as the U.S. Forest Service's Smokey the Bear campaign, and that the focus should be on making kids "responsible cyber-citizens." While some states, including Virginia, have created online education requirements, Thierer said more could be done with a nationwide effort. "I think we need that kind of program at the Federal level." -- Andrew Feinberg

95 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 11, 2008 Wednesday

LENGTH: 533 words**HEADLINE:** Tate Concerned about Kids' Use of Convergence Devices, Streaming Content**BODY:**

Interactive media present a new set of risks to children, FCC Commissioners Deborah Tate and Jonathan Adelstein said at the PointSmart.ClickSafe Summit. In separate keynotes, the commissioners said the issues require attention to ensure that children remain safe in a broadband-connected world.

Saying she would rather discuss issues than statistics, Tate said the Internet is becoming a part of everyday life for kids and teens, and "what was once considered and described as a virtual world... is now our children's very real world." This expansion, Tate said, has brought to light a new set of risks that young people face in their online lives. The Internet is becoming more important to young people, she said, noting that kids now are creating their own content on video sharing and social networking site. She said the phenomenon presents even greater dangers as kids share personal information and photographs through social networks.

Cyberbullying is Tate's latest interest; it was piqued by the recent Megan Meier case (WID May 19 p6). Citing statistics that show one in four children have experienced some kind of cyberbullying, Tate said her strong feelings on the issue come from her experience "as a mother...and as a policymaker." Tate said cyberbullying is not only a technological issue but a health and welfare threat.

Convergence and the near-ubiquity of the Internet on mobile phones make parental and educational involvement even more important, Tate said. She also urged the cable and wireless industries to help create a safe environment for young people.

Adelstein said protecting children in the virtual world is not dissimilar from the real world, stressing parental involvement as the first line of defense. He said a major threat to children's online mental and physical health comes from TV as well as the Internet. One danger that's being overlooked on both TV and the Internet, he said, is "excessive commercialism for unhealthy products." He called parents the "first, last, and best line of defense against all forms of objectionable content" and praised industry efforts to increase online literacy. However, he said some problems by their very nature can be solved only by regulation, even if the regulations are unpopular among companies: "It's another thing entirely to take real action that can make a difference."

Convergence of TV and the Internet poses further dangers to children in the form of commercials, Adelstein said, as interactive media begin to contain more and more advertising content. Adelstein criticized recently passed media ownership rules, saying excessive commercialization is a consequence of consolidation. He urged Martin to issue a final rule banning interactive advertising to children, and expressed hope that his colleagues would support it.

Just because interactive TV is new doesn't mean it's too soon to act, Adelstein said. Referencing a Kaiser study on online food advertising, and a recent Washington Post series on childhood obesity, he said "we know what is going to

happen," and that if the Commission doesn't act on interactive advertising to children before it becomes well established, "it could be too late." - Andrew Feinberg

97 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

June 10, 2008 Tuesday

LENGTH: 601 words**HEADLINE:** Net Neutrality, First Amendment Closely Linked, ACLU Members Told**BODY:**

Internet users must remain vigilant and push Congress and the FCC to protect a free and open network, said a group of privacy and net neutrality advocates during a Monday panel at the ACLU Membership Conference in Washington, D.C. An open information highway starts with the on-ramps, said Public Knowledge's Gigi Sohn, who presented as her goal a world where "people like you and me can use any device, and any application" on networks.

Open platforms should be extended to wireless networks, Sohn said. Wireless carriers haven't been required to adhere to Carterfone "right to attach" rules, Sohn said. But she said the spread of VoIP software for smartphone devices and the buildout of 3G data networks have painted the Big Four providers into a corner as VoIP companies offer call quality on a par with PCS service and lower per-minute costs. VoIP provider Skype has filed a petition to apply Carterfone to the currently operational networks, but FCC Chairman Kevin Martin announced he would circulate an order to dismiss the request.

Cable companies and incumbent telcos control 96 percent of the broadband service in the U.S., Sohn said, and they can monitor what kind of data flows through their networks, control what happens to it and track who views it. Only net neutrality rules can check these capabilities, she said.

Neutrality requires close attention to protecting privacy, said Melissa Ngo, publisher of PrivacyLives.com. Deep packet inspection technology can capture and potentially store user data, build individualized profiles of Web usage and monitor communications for governments, she said. Taking the technology a step further, she said, are particular onerous plans announced by Charter Communications and NebuAd to target ads to their 2.8 million subscribers. House Telecommunications Subcommittee Chairman Edward Markey, D- Mass., and Ranking Member Joseph Barton, R-Texas, have sent letters to Charter asking for details on the program, which the company has since put on hold.

Deep packet inspection can be used by anyone operating on the network, Ngo said. Of particular concern are search engines and e-mail providers such as Google, Yahoo and AOL, she said, because they collect massive histories of users' search queries as well as communications. Of the three, Google does the most deep packet inspections -- the heart of the contextual advertising system that produces most of the company's revenue, she said.

The most prominent victim of deep packet inspection could be the First Amendment, said ACLU policy counsel Jim Tucker. Noting that the broadband industry routinely asserts First Amendment protection against net neutrality proposals while going out of their way to allow government to monitor customer communications. He expressed alarm at the potential harm to free speech that deep packet inspection could cause if used by government to censor speech, as suggested by several child protection and "homegrown terrorism" bills before Congress, or to block lawful services for private economic gain by "nonstate actors."

Tucker said broadband providers, which also sell phone service, have an economic incentive to degrade and block competing services like Skype and Vonage. He recalled how AOL once blocked an e-mail petition against a new fee it intended to charge. "When an ISP doesn't like the content of a message... they respond by blocking it." Warning about the proposed M2Z free wireless broadband service and its filtering provisions, he suggested the only way to get rid of the mandatory content filter would be to pay for a premium service. - Andrew Feinberg

98 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 10, 2008 Tuesday
Correction Appended

LENGTH: 1000 words

HEADLINE: Net Neutrality, First Amendment Closely Linked, ACLU Members Told

BODY:

Internet users must remain vigilant and push Congress and the FCC to protect a free and open network, said a group of privacy and net neutrality advocates during a Monday panel at the ACLU Membership Conference in Washington, D.C. An open information highway starts with the on-ramps, said Public Knowledge's Gigi Sohn, who presented as her goal a world where "people like you and me can use any device, and any application" on networks.

Open platforms should be extended to wireless networks, Sohn said. Wireless carriers haven't been required to adhere to Carterfone "right to attach" rules, Sohn said. But she said the spread of VoIP software for smartphone devices and the buildout of 3G data networks have painted the Big Four providers into a corner as VoIP companies offer call quality on a par with PCS service and lower per-minute costs. VoIP provider Skype has filed a petition to apply Carterfone to the currently operational networks, but FCC Chairman Kevin Martin announced he would circulate an order to dismiss the request.

Cable companies and incumbent telcos control 96 percent of the broadband service in the U.S., Sohn said, and they can monitor what kind of data flows through their networks, control what happens to it and track who views it. Only net neutrality rules can check these capabilities, she said.

Neutrality requires close attention to protecting privacy, said Melissa Ngo, publisher of PrivacyLives.com. Deep packet inspection technology can capture and potentially store user data, build individualized profiles of Web usage and monitor communications for governments, she said. Taking the technology a step further, she said, are particular onerous plans announced by Charter Communications and NebuAd to target ads to their 2.8 million subscribers. House Telecom Subcommittee Chairman Edward Markey, D-Mass., and Ranking Member Joe Barton, R-Texas, have sent letters to Charter asking for details on the program, which the company has since put on hold.

Deep packet inspection can be used by anyone operating on the network, Ngo said. Of particular concern are search engines and e-mail providers such as Google, Yahoo and AOL, she said, because they collect massive histories of users' search queries as well as communications. Of the three, Google does the most deep packet inspections -- the heart of the contextual advertising system that produces most of the company's revenue, she said.

The most prominent victim of deep packet inspection could be the First Amendment, said ACLU policy counsel Jim Tucker. Noting that the broadband industry routinely asserts First Amendment protection against net neutrality proposals while going out of their way to allow government to monitor customer communications. He expressed alarm at the potential harm to free speech that deep packet inspection could cause if used by government to censor speech, as suggested by several child protection and "homegrown terrorism" bills before Congress, or to block lawful services for private economic gain by "nonstate actors."

Tucker said broadband providers, which also sell phone service, have an economic incentive to degrade and block competing services like Skype and Vonage. He recalled how AOL once blocked an e-mail petition against a new fee it intended to charge. "When an ISP doesn't like the content of a message... they respond by blocking it." Warning about the proposed M2Z free wireless broadband service and its filtering provisions, he suggested the only way to get rid of the mandatory content filter would be to pay for a premium service. - Andrew Feinberg

ACLU Membership Conference Notebook...

Electronic surveillance legislation probably won't budge until August, ranking Senate Judiciary Committee member Arlen Specter, R-Pa., told the ACLU Membership Conference on Monday. Negotiations have stalled over Republican efforts to pass a bill (S-2248) giving phone companies retroactive immunity for their purported roles in President Bush's post- Sept. 11 surveillance program. The House has balked at the bill, which reflects a deal between the White House and the Senate Intelligence Committee. The program, a trigger for numerous lawsuits challenging its legality, wouldn't have come to light without newspaper reports, Specter told the ACLU conference. Former New York Times reporter James Risen, among reporters who broke the story, told the conference that the White House threatened his publisher with a court injunction in its effort to keep the story from running. "The president told him he would have blood on his hands if he published this story," Risen said. "That's a heavy burden for a newspaper person." Specter called Bush's policy a "vast expansion of executive authority" that has gone too far. He said neither the courts nor Congress have acted to stop it. "I regret congressional oversight has been, in my judgment, totally insufficient." Specter differs from many GOP colleagues in his resistance to full retroactive immunity. "It's difficult to give immunity when you don't know what you're granting retroactive immunity for," Specter said. He supports a proposal to substitute the government for phone companies in lawsuits, to allow courts to review the Bush program's legal underpinnings while taking the pressure off companies. "The critical factor is to get the judicial review," Specter said. "The question of who pays" if the program is found to have violated Americans' privacy is secondary, he said. The substitution, voted down by the Judiciary Committee when Specter offered it as an amendment to a Judiciary surveillance bill, offers a way to assure civil-liberties advocates that proper process is being followed, Specter said. Intelligence Committee ranking member Kit Bond, R-Mo., has proposed a compromise to S-2248 that would put Foreign Intelligence Surveillance Court judges in charge of reviewing the program. The ACLU opposes that approach. In meetings on the Hill this week, the group plans to fight immunity efforts. -- AV

CORRECTION-DATE: July 15, 2008

CORRECTION:

We mistakenly attributed to PrivacyLives.com's Melisso Ngo the statement that Google's revenue depends heavily on deep-packet inspection (WID June 10 p3); it was based on our own research...

99 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 10, 2008 Tuesday

LENGTH: 1075 words**HEADLINE:** Facebook International Expansion Highlights Privacy Issues**BODY:**

American Internet experts and analysts disagree on a Canadian privacy group's complaint against Facebook, filed May 30 before the Canadian Privacy Commissioner (WID June 2 p2). Some want the U.S. to pass its own privacy protection law. Others say the Canadian privacy commissioner's response to the complaint could lead to international gridlock, should a patchwork of contradictory national privacy laws emerge.

Facebook Chief Privacy Officer Chris Kelly attacked the complaint's reasoning in a statement issued the same day as the complaint was filed. Facebook users are "willingly sharing" data, Kelly said. His claim was challenged by BT Chief Security and Technology Officer Bruce Schneier. "I'm pretty sure if you spoke to any seven people who use Facebook, they would never say the point of it is to share information," Schneier said in an interview. "It's all about connecting with their friends."

Facebook default settings are a major security concern, Schneier said, agreeing with the Canadian Internet Public Policy and Information Clinic filing. Data show that half of people won't change default settings, especially on social networking sites like Facebook, he said: "Most people will do what's normal." The best privacy practice would be for people to have to choose actively what to share, rather than having the ability to choose what not to share, he said.

Control over user information is a major issue for social networks, Schneier said. Referring to a user revolt over Facebook's Beacon feature, he traced the outcry not to the sharing of information, but to doing so without permission. "Who's in charge of my information?" he asked. "That's really what the concerns are." In its terms of service Facebook claims ownership of all user data on the site, which Schneier explained as driven by an economic motive to "lock in" users: "They want to make it painful for you to leave."

The U.S. needs a comprehensive data privacy law, Schneier said, noting that Facebook's questionable privacy practices are getting their first test before a foreign regulatory body. The U.S. lags far behind many countries at protecting people's data, he said: "We really need the same sorts of protection that Canada has."

Others said users should know what they are getting into, calling terms of service and privacy policies sufficient protection against abuse. Schneier and those who share his views err by "turning this into a moral issue," Berin Szoka of the Progress and Freedom Foundation said. Szoka contested many aspects of the Canadian law, characterizing them as potentially harmful if implemented in the U.S.

One point of contention is Facebook's policy of retaining user data after a user deletes his or her account without asking explicitly that data associated with it be deleted. CIPPIC terms this practice misleading and illegal. Facebook said it wants exiting users to be able to restore accounts if they rejoin. Szoka called the practice reasonable for any hosted online service. He expressed his own worry at having a malicious user delete an account: "I live in fear that

someone might break into my Gmail account and delete it, and it would be gone forever."

Szoka's view doesn't jibe with Google policy, however. Google's official Gmail FAQ page says the company "keeps multiple backup copies of users' e-mails so that we can recover messages and restore accounts in case of errors or system failure." However, unlike Facebook, which indefinitely keeps from deleted accounts, Google retains backups for a limited amount of time: "We will make reasonable efforts to remove deleted information from our systems as quickly as is practical."

Szoka is more troubled by the implication that "Canada is trying to extend its privacy laws to other countries," he said. Mandatory default opt-out for sharing data could have "real world consequences," he added. He said a patchwork of U.S. state laws isn't ideal, but to adopt a system similar to Canada's would be "to buy into some comprehensive, onerous federal legislation." And were Facebook to revise its site to obey Canadian law, such as by not demanding registrants' birthdates, it could break U.S. laws. These include child protection statutes that require sites to ask users' ages before providing service.

Facebook deems user privacy a high priority, it said. In a March 10 developer Q&A session, founder and CEO Mark Zuckerberg was asked about sharing data with governments. "Making sure people's information is private" is one of his company's major goals, and Facebook would avoid putting itself in a position where obeying the law would compromise privacy, Zuckerberg said: "Keeping people's private information only accessible to people they want to share it with is a core thing for Facebook."

User feedback has led to gradual introduction of more granular privacy controls, but Facebook privacy settings still default to sharing most information. However, in what may be an attempt to neutralize aspects of the CIPPIC complaint, a login timeout feature such as online banking sites use has been deployed quietly. That functionality's previous absence figured prominently in the CIPPIC filing.

The complaint may be an opening salvo over international legal issues involving Facebook. In the same March Q&A, a questioner asked how Facebook would handle information sharing with authoritarian governments, citing an episode in which Yahoo allegedly shared data leading to a Chinese blogger's arrest.

Zuckerberg said at the time that as yet Facebook hadn't expanded into China because "we're not openly working with governments." But in countries where Facebook does operate, "we have to follow the law," he added. The company's China strategy was mired in intense internal debate over whether to launch using servers located there, he said. That would mean better service but could put employees at risk, whereas using outside servers could be blocked or slowed by the government, he said.

Zuckerberg then hesitated to commit to a firm China strategy, describing the available options as "not a great set of tradeoffs." But a source familiar with Facebook operations said the company plans to launch a Chinese network "as soon as the site is translated." Repeated calls and e-mails to Kelly, Zuckerberg and Adam Conner, Facebook's Washington, D.C.-based associate for privacy and global public policy requesting comments on these issues were not returned at our deadline. - Andrew Feinberg

100 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 10, 2008 Tuesday
Correction Appended

LENGTH: 1000 words

HEADLINE: Net Neutrality, First Amendment Closely Linked, ACLU Members Told

BODY:

Internet users must remain vigilant and push Congress and the FCC to protect a free and open network, said a group of privacy and net neutrality advocates during a Monday panel at the ACLU Membership Conference in Washington, D.C. An open information highway starts with the on-ramps, said Public Knowledge's Gigi Sohn, who presented as her goal a world where "people like you and me can use any device, and any application" on networks.

Open platforms should be extended to wireless networks, Sohn said. Wireless carriers haven't been required to adhere to Carterfone "right to attach" rules, Sohn said. But she said the spread of VoIP software for smartphone devices and the buildout of 3G data networks have painted the Big Four providers into a corner as VoIP companies offer call quality on a par with PCS service and lower per-minute costs. VoIP provider Skype has filed a petition to apply Carterfone to the currently operational networks, but FCC Chairman Kevin Martin announced he would circulate an order to dismiss the request.

Cable companies and incumbent telcos control 96 percent of the broadband service in the U.S., Sohn said, and they can monitor what kind of data flows through their networks, control what happens to it and track who views it. Only net neutrality rules can check these capabilities, she said.

Neutrality requires close attention to protecting privacy, said Melissa Ngo, publisher of PrivacyLives.com. Deep packet inspection technology can capture and potentially store user data, build individualized profiles of Web usage and monitor communications for governments, she said. Taking the technology a step further, she said, are particular onerous plans announced by Charter Communications and NebuAd to target ads to their 2.8 million subscribers. House Telecom Subcommittee Chairman Edward Markey, D-Mass., and Ranking Member Joe Barton, R-Texas, have sent letters to Charter asking for details on the program, which the company has since put on hold.

Deep packet inspection can be used by anyone operating on the network, Ngo said. Of particular concern are search engines and e-mail providers such as Google, Yahoo and AOL, she said, because they collect massive histories of users' search queries as well as communications. Of the three, Google does the most deep packet inspections -- the heart of the contextual advertising system that produces most of the company's revenue, she said.

The most prominent victim of deep packet inspection could be the First Amendment, said ACLU policy counsel Jim Tucker. Noting that the broadband industry routinely asserts First Amendment protection against net neutrality proposals while going out of their way to allow government to monitor customer communications. He expressed alarm at the potential harm to free speech that deep packet inspection could cause if used by government to censor speech, as suggested by several child protection and "homegrown terrorism" bills before Congress, or to block lawful services for private economic gain by "nonstate actors."

Tucker said broadband providers, which also sell phone service, have an economic incentive to degrade and block competing services like Skype and Vonage. He recalled how AOL once blocked an e-mail petition against a new fee it intended to charge. "When an ISP doesn't like the content of a message... they respond by blocking it." Warning about the proposed M2Z free wireless broadband service and its filtering provisions, he suggested the only way to get rid of the mandatory content filter would be to pay for a premium service. - Andrew Feinberg

ACLU Membership Conference Notebook...

Electronic surveillance legislation probably won't budge until August, ranking Senate Judiciary Committee member Arlen Specter, R-Pa., told the ACLU Membership Conference on Monday. Negotiations have stalled over Republican efforts to pass a bill (S-2248) giving phone companies retroactive immunity for their purported roles in President Bush's post- Sept. 11 surveillance program. The House has balked at the bill, which reflects a deal between the White House and the Senate Intelligence Committee. The program, a trigger for numerous lawsuits challenging its legality, wouldn't have come to light without newspaper reports, Specter told the ACLU conference. Former New York Times reporter James Risen, among reporters who broke the story, told the conference that the White House threatened his publisher with a court injunction in its effort to keep the story from running. "The president told him he would have blood on his hands if he published this story," Risen said. "That's a heavy burden for a newspaper person." Specter called Bush's policy a "vast expansion of executive authority" that has gone too far. He said neither the courts nor Congress have acted to stop it. "I regret congressional oversight has been, in my judgment, totally insufficient." Specter differs from many GOP colleagues in his resistance to full retroactive immunity. "It's difficult to give immunity when you don't know what you're granting retroactive immunity for," Specter said. He supports a proposal to substitute the government for phone companies in lawsuits, to allow courts to review the Bush program's legal underpinnings while taking the pressure off companies. "The critical factor is to get the judicial review," Specter said. "The question of who pays" if the program is found to have violated Americans' privacy is secondary, he said. The substitution, voted down by the Judiciary Committee when Specter offered it as an amendment to a Judiciary surveillance bill, offers a way to assure civil-liberties advocates that proper process is being followed, Specter said. Intelligence Committee ranking member Kit Bond, R-Mo., has proposed a compromise to S-2248 that would put Foreign Intelligence Surveillance Court judges in charge of reviewing the program. The ACLU opposes that approach. In meetings on the Hill this week, the group plans to fight immunity efforts. -- AV

CORRECTION-DATE: July 15, 2008

CORRECTION:

We mistakenly attributed to PrivacyLives.com's Melisso Ngo the statement that Google's revenue depends heavily on deep-packet inspection (WID June 10 p3); it was based on our own research...

101 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 10, 2008 Tuesday

LENGTH: 1075 words**HEADLINE:** Facebook International Expansion Highlights Privacy Issues**BODY:**

American Internet experts and analysts disagree on a Canadian privacy group's complaint against Facebook, filed May 30 before the Canadian Privacy Commissioner (WID June 2 p2). Some want the U.S. to pass its own privacy protection law. Others say the Canadian privacy commissioner's response to the complaint could lead to international gridlock, should a patchwork of contradictory national privacy laws emerge.

Facebook Chief Privacy Officer Chris Kelly attacked the complaint's reasoning in a statement issued the same day as the complaint was filed. Facebook users are "willingly sharing" data, Kelly said. His claim was challenged by BT Chief Security and Technology Officer Bruce Schneier. "I'm pretty sure if you spoke to any seven people who use Facebook, they would never say the point of it is to share information," Schneier said in an interview. "It's all about connecting with their friends."

Facebook default settings are a major security concern, Schneier said, agreeing with the Canadian Internet Public Policy and Information Clinic filing. Data show that half of people won't change default settings, especially on social networking sites like Facebook, he said: "Most people will do what's normal." The best privacy practice would be for people to have to choose actively what to share, rather than having the ability to choose what not to share, he said.

Control over user information is a major issue for social networks, Schneier said. Referring to a user revolt over Facebook's Beacon feature, he traced the outcry not to the sharing of information, but to doing so without permission. "Who's in charge of my information?" he asked. "That's really what the concerns are." In its terms of service Facebook claims ownership of all user data on the site, which Schneier explained as driven by an economic motive to "lock in" users: "They want to make it painful for you to leave."

The U.S. needs a comprehensive data privacy law, Schneier said, noting that Facebook's questionable privacy practices are getting their first test before a foreign regulatory body. The U.S. lags far behind many countries at protecting people's data, he said: "We really need the same sorts of protection that Canada has."

Others said users should know what they are getting into, calling terms of service and privacy policies sufficient protection against abuse. Schneier and those who share his views err by "turning this into a moral issue," Berin Szoka of the Progress and Freedom Foundation said. Szoka contested many aspects of the Canadian law, characterizing them as potentially harmful if implemented in the U.S.

One point of contention is Facebook's policy of retaining user data after a user deletes his or her account without asking explicitly that data associated with it be deleted. CIPPIC terms this practice misleading and illegal. Facebook said it wants exiting users to be able to restore accounts if they rejoin. Szoka called the practice reasonable for any hosted online service. He expressed his own worry at having a malicious user delete an account: "I live in fear that

someone might break into my Gmail account and delete it, and it would be gone forever."

Szoka's view doesn't jibe with Google policy, however. Google's official Gmail FAQ page says the company "keeps multiple backup copies of users' e-mails so that we can recover messages and restore accounts in case of errors or system failure." However, unlike Facebook, which indefinitely keeps from deleted accounts, Google retains backups for a limited amount of time: "We will make reasonable efforts to remove deleted information from our systems as quickly as is practical."

Szoka is more troubled by the implication that "Canada is trying to extend its privacy laws to other countries," he said. Mandatory default opt-out for sharing data could have "real world consequences," he added. He said a patchwork of U.S. state laws isn't ideal, but to adopt a system similar to Canada's would be "to buy into some comprehensive, onerous federal legislation." And were Facebook to revise its site to obey Canadian law, such as by not demanding registrants' birthdates, it could break U.S. laws. These include child protection statutes that require sites to ask users' ages before providing service.

Facebook deems user privacy a high priority, it said. In a March 10 developer Q&A session, founder and CEO Mark Zuckerberg was asked about sharing data with governments. "Making sure people's information is private" is one of his company's major goals, and Facebook would avoid putting itself in a position where obeying the law would compromise privacy, Zuckerberg said: "Keeping people's private information only accessible to people they want to share it with is a core thing for Facebook."

User feedback has led to gradual introduction of more granular privacy controls, but Facebook privacy settings still default to sharing most information. However, in what may be an attempt to neutralize aspects of the CIPPIC complaint, a login timeout feature such as online banking sites use has been deployed quietly. That functionality's previous absence figured prominently in the CIPPIC filing.

The complaint may be an opening salvo over international legal issues involving Facebook. In the same March Q&A, a questioner asked how Facebook would handle information sharing with authoritarian governments, citing an episode in which Yahoo allegedly shared data leading to a Chinese blogger's arrest.

Zuckerberg said at the time that as yet Facebook hadn't expanded into China because "we're not openly working with governments." But in countries where Facebook does operate, "we have to follow the law," he added. The company's China strategy was mired in intense internal debate over whether to launch using servers located there, he said. That would mean better service but could put employees at risk, whereas using outside servers could be blocked or slowed by the government, he said.

Zuckerberg then hesitated to commit to a firm China strategy, describing the available options as "not a great set of tradeoffs." But a source familiar with Facebook operations said the company plans to launch a Chinese network "as soon as the site is translated." Repeated calls and e-mails to Kelly, Zuckerberg and Adam Conner, Facebook's Washington, D.C.-based associate for privacy and global public policy requesting comments on these issues were not returned at our deadline. - Andrew Feinberg

102 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 06, 2008 Friday

LENGTH: 514 words**HEADLINE:** EFF Sides with MySpace Against Local Official in Illinois**BODY:**

MySpace shouldn't be required to reveal the identities of anonymous authors of MySpace profiles criticizing a municipal leader in Illinois, the Electronic Frontier Foundation told the Cook County, Ill., Circuit Court. EFF filed an amicus brief Thursday on behalf of MySpace, citing constitutional and statutory protections for anonymous speech and electronic records.

The case centers on MySpace pages purportedly belonging to Larry Dominick, the town president of Cicero, Ill. Private attorneys paid with tax money have asked on Dominick's behalf that the judge order MySpace to provide information to identify the anonymous authors of the profiles. The petition, filed before any legal complaint in the case, alleges they were "false and defamatory." The profiles weren't available Thursday on MySpace and the petition didn't specify the material that Dominick objected to.

The compliance office at MySpace hasn't received the petition, said EFF senior staff attorney Matt Zimmerman, one of the brief's authors. He called troubling the procedure that Dominick's attorneys are using, because the profiles' authors aren't being notified of the request. The EFF brief compares the tactic to those used by the RIAA to identify anonymous file-sharers, a legal strategy which Federal courts have said raises serious questions on the use of a civil subpoena to strip away anonymity protected by the First Amendment.

Dominick is suing in his capacity as town president. In a May 2007 statement to the Chicago Tribune, town spokesman Dan Proft said this was because the profiles were tied to his job. Proft said the profiles contained "silly juvenile stuff, but it was defamatory... We want to know who is responsible so we can go after them." He said the profiles were "not a parody or a critique of performance" but "a libelous statement against a public official."

Filing in an official capacity makes Dominick even less entitled to the information, according to the EFF's brief, which cites the 1986 U.S. Stored Communications Act as barring government bodies from obtaining identify information in civil discovery. The law prohibits disclosure of customer records to governmental bodies by an electronic service provider such as MySpace.

Even if the Dominick had filed in his personal capacity, Zimmerman argued in the brief, the anonymous authors enjoy First Amendment protection from disclosure of their identities. He said the First Amendment requires a much higher burden of proof of defamation than for other plaintiffs when a public figure is involved.

Arguments on the petition are scheduled "in the next week or so" according to Brian Saucier, an attorney representing Dominick. Saucier wouldn't comment on whether he was being paid from city coffers or discuss the content of the alleged defamatory statements, instead saying they would be placed in the record "when we file a defamation action." Saucier then qualified his statement by saying the profiles would be made public "if and when we

file." He wouldn't discuss the constitutional and policy matters involved. - Andrew Feinberg

104 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 04, 2008 Wednesday

LENGTH: 464 words**HEADLINE:** Government Using Web 2.0 Innovations to Gauge Feedback**BODY:**

The new dark blue uniforms recently unveiled at BWI Airport's TSA checkpoints didn't result from an expensive study by consultants or a systematic plan by managers, said Stephen Goldsmith, a professor at Harvard's Kennedy School of Government. Instead, Goldsmith told the audience Tuesday at a Deloitte-sponsored seminar on Web 2.0 in Government, the new outfits came in response to comments by employees and travelers on Evolution of Security, the TSA blog.

Seminar attendees heard a series of such stories of great successes -- and miserable failures -- in using technology to improve the work of government agencies. Goldsmith and Frank DiGiammarino, vice president for strategic initiatives at the National Academy of Public Administration, gave examples of how Web 2.0 technology can improve service and make employees happier and more productive -- in addition to a few embarrassing failures caused by using technology to "improve" service without listening to the recipients of the services.

Effective use of technology can increase civic involvement, Goldsmith said. He cited Minneapolis, which adopted a wiki for residents to comment on zoning and land use plans, after a new city park built a basketball court that no one wanted. The wiki, he said, attracted far more attention and was much more productive than a community meeting. Goldsmith, a former two-term mayor of Indianapolis, said the town-hall meetings he remembered always resulted in the loudest voices drowning out all others. Wikis are collaborative, allowing for more-constructive discussion over a longer periods, with results more satisfying for all involved, he said.

Collaborative communities like wikis can produce better results than experts, Goldsmith said. He told of a city engineer's decision to repave a section of sidewalk that served mainly as an open-air drug market, while less damaged but more heavily traveled sections were left alone until the engineers determined they needed repair. If the city had been able to monitor community feedback, he said, it might have avoided the subsequent outcry over spending public money to repair a drug corner instead of maintaining the sidewalk outside a church.

DiGiammarino said collaborative Web 2.0 tools allow better use of time and can save money. He said the TSA blog, allowing interaction among the agency, its employees and "customers," is a textbook example of the value of management embracing Web 2.0.

The blog, DiGiammarino said, was an example of how collecting feedback in an open setting allowed for more efficient operation and quicker response to concerns from an organization with 43,000 front-line employees who screen millions of passengers a day. Comments on the blog resulted in 20 successful policy changes in six months. - Andrew Feinberg

106 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

June 02, 2008 Monday

LENGTH: 528 words**HEADLINE:** Facebook Cited in Canadian Privacy Commissioner Complaint**BODY:**

Facebook faces a complaint filed Friday with the Canadian Privacy Commissioner by the University of Ottawa's Canadian Internet Policy and Public Interest Clinic. CIPPIC charges Facebook with violating the Personal Information Protection and Electronic Documents Act, including not fully disclosing how the social networking site uses personal data it collects and shares, not deleting personal material automatically when an account is closed and lack of transparency on how user data are tracked by or shared with advertisers.

CIPPIC Director Phillipa Lawson said Facebook's most troubling problems include situations in which the service gives users no choice when giving third-party applications access to information, specifically that "there is no way to uncheck the box" and revoke permissions. Lawson also cited Facebook's contact importer, which searches users' e-mail address books to connect them with contacts already on the service. The tool allows users to invite contacts to join Facebook, and by default invites all of a user's contacts, but Facebook doesn't disclose what it does with addresses to which invitations are not sent.

Facebook's account termination policy violates Canadian law, the complaint alleges. Now, when a user "terminates" an account, Facebook merely deactivates it, retaining the user's personal information and other data. Facebook permanently deletes account data only when the departing user specifically requests that by e-mail.

The complaint also questions the legality of Facebook's assertion of ownership of all user data, and site security features, citing Facebook's lack of an automatic log-off feature similar to online banking sites.

Facebook Chief Privacy Officer Chris Kelly shrugged off the complaint, saying Facebook takes users' privacy seriously. "At Facebook, we pride ourselves on the industry-leading controls we offer users over their personal information," he said in a written statement. Kelly also said the complaint has "serious factual errors" and nearly all data is "willingly shared by users."

Lawson questioned Kelly's definition of "willingly" and said the most disturbing aspect of problems with Facebook are evident in the site's privacy settings, which default to sharing information. She said Facebook would be in a much stronger position if the setting was changed.

Facebook has faced many privacy controversies, lately over last year's Beacon advertising feature. "Most of the points here have been raised with Facebook in the past," Lawson said. -- Andrew Feinberg

* * * * Facebook is blocking messages that link to sites with "contact importer" applications and catching flak from users, Facebook security engineer Ryan McGeehan said last week on the Facebook blog. The curbs aim to protect Facebook users' privacy and that of their friends, he said. Users providing Facebook login information to a site with a contact importer not only "spam all of their friends" but grant full control of their Facebook accounts to such

applications, McGeehan said. Users will be able to share their information with other sites through "trusted authentication" in Facebook's nascent Connect initiative, he said.

108 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

May 29, 2008 Thursday

LENGTH: 845 words**HEADLINE:** Online Risks to Children, Teens Called Often Exaggerated**BODY:**

Results of a 2005 study on online risks to youth are routinely exaggerated, misquoted or used out of context by government officials and child advocates, said researchers and online safety experts. The often-quoted statistic that "1 in 7 children are sexually solicited online" comes from a University of New Hampshire study paid for by the National Center for Missing and Exploited Children. Despite repeated statements by the study's authors and publication of a fact sheet that suggests using one in 25 as a more accurate figure, the Center continues to use one in seven in its print materials and TV ads.

The most common misinterpretation of the study is the assumption that the one out of seven children it concludes have been solicited were approached by predators. According to Kimberly Mitchell, co-author and research assistant professor at the university, the ratio refers to "the number of kids who are solicited online" -- but in most cases the solicitors were other youths and the definition of solicitation was very broad. Even very few of the most aggressive cases resulted in contact, she said. Mitchell expressed concern that the study is being used in ways that don't reflect the real risks to children and teens. For example, the Web page for Florida Attorney General Bill McCollum's Child Predator CyberCrime Unit says, "Nationally, one in seven children between the ages of ten and 17 have been solicited online by a sexual predator."

The setting in which the numbers are used also can mislead. During last week's NCTA convention in New Orleans, FCC Commissioner Deborah Tate repeated the one in seven figure in a speech on the importance of protecting children from online predators. Tate didn't respond to questions about the study authors' desire for more accurate use of the data. When presented with their fact sheet, she reacted angrily, refusing to read it, saying, "We can quibble all we want to about statistics." She insisted that the numbers reflected actual predators preying on children. "To me it doesn't matter whether it's one in 100," Tate said. "I'm going to continue to talk about this."

Tate's use of "one in seven was probably inappropriate," Mitchell said, if the commissioner was talking about online predators. Instead, she said, child safety advocates should use the one in 25 number, which refers to more aggressive incidents that threaten to move offline. Mitchell expressed frustration over frequent "twisting" of the data, saying the results are often used to fit agendas.

Center Justifies its Numbers

NCMEC President Ernie Allen said his organization hasn't used the one in seven ratio in reference to predators. Allen said the center uses the statistic as a "wake-up call." He insisted that the center balances its desire to educate with the need for accuracy. "One in seven is a real number. We use it in context, and frankly, it's a number we're concerned about."

Allen acknowledged the data didn't correspond to actual harm by Internet predators, but "thousands of kids" had been lured away "by a variety of means." He stood by "one in seven" as a "demonstrator of the fact that... there are those online who are doing a variety of things that are inappropriate."

Pressed about the researcher's fact sheet, Allen said he welcomed the clarification, but nevertheless stood by the use "one in seven." He said he believes that the number of youths being preyed upon is actually underestimated, citing his observations of police decoy stings.

The one in seven ratio is probably low, said Lieutenant Brett Butler of the Arlington County, Va., Police Department Special Victims Unit. Butler said the problem is so severe that he has devoted two detectives to investigating online predation. He said his decoy operations are like "putting blood in the water for a shark." The vast majority of crimes his detectives see are committed by older adults going after decoys posing as 11 to 13 year old girls and boys, Butler said, and the crimes involve long-term grooming and planning by the perpetrators.

Other online safety advocates disagree with use of the one in seven number. Larry Magid, founder of ConnectSafely.org, said citing an out-of-context statistic is inappropriate. Magid disagreed with the routine use of the figure, saying that though it makes a good sound bite for a political campaign or in a push for funding, continued exaggeration of online dangers is a problem and is "a form of grandstanding and fear mongering that can be useful in a political context."

Online safety efforts should focus on high-risk groups, Magid said. Referring to the original university study and a new paper by its authors in the March issue of American Psychologist, he said "the data is clear" and very few solicitations were "an adult seeking a child for sexual exploitation." He suggested that child safety advocates should spend more time reaching out to groups at highest risk for online exploitation, which according to University of New Hampshire researcher Janis Wolak are the same as those at risk in general. -- Andrew Feinberg

110 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

May 21, 2008 Wednesday

LENGTH: 1205 words**HEADLINE:** Chrysler Exec.: Cable needs Targeted Advertising**BODY:**

NEW ORLEANS --- Targeted advertising technology is the only way for cable to adapt to a fragmented advertising market, Chrysler Chief Marketing Officer Deborah Meyer told a Cable Ad Bureau general session at the NCTA Convention here. Separately, top cable and network programming officials said it's time for cable to start making money, through national ad ventures like Project Canoe, on VoD offerings until now largely free. Otherwise, they said, they'll never make good on VoD's vast ad potential and industry will keep seeing ad dollars flow to the Internet.

While cable is still Chrysler's top advertising partner, Meyer said the automaker's marketing budget is shifting toward the Internet because of the medium's ability to track and target different ads to different kinds of consumers, then measure customer response. Meyer said Chrysler is "moving away from traditional marketing where you establish one idealized target," and that cable needs to adapt to the new narrowcasting strategy.

Meyer was optimistic about cable's chances to succeed in the new market, saying "we should be able to use that same model with the technology that cable is developing." She disagreed that market fragmentation is a negative, saying fragmentation can provide the industry with opportunities to place ads in front of specific target demographics. Calling for increased deployment of addressable advertising technology, Meyer said advertisers, as customers, want to "deliver one message to the married 55-year-old man watching Battlestar Galactica, and a very different message to the 25-year-old single woman watching the same show."

Industry executives were optimistic about the potential of targeted and addressable ads, despite some disagreement about the state of the market environment. Naked Communications CEO Paul Woolmington said the ad market is going through a "seismic, but slow shift" and that advertising customers in all industries "want to get much closer to the point of decision making."

The rise of targeted and interactive media is not an either/or situation, said Tony Vinciguerra of Fox Networks, who compared today's environment to the advent of TV during the radio age, and the addition of radio to newspapers before that. "Nothing is going away," he said. Cox Communications President Paul Esser said the trend toward measurability and accountability of targeting presents "huge opportunities" for the industry.

Despite the competition, cable benefits from a majority of Chrysler's ad buys, Meyer said. However, she warned that because of the need to target and do more in an uncertain economy, dollars are moving further and further into the local markets and the Internet. Meyer said dealer groups are looking for the ability to deliver multiple messages, and the current model "just doesn't work for them."

DVR and VOD technology is providing a stop-gap solution, Vinciguerra said, saying DVR lets advertisers see how many customers watch commercials and how to maximize those viewers. When asked about DirecTV's 30-second skip

feature, he said not all consumers use DVRs the same way, and older consumers don't skip commercials. Regarding Cablevision's ill-fated network DVR technology, COO Tom Rutledge said the content providers' campaign against the network DVR system was a lost opportunity and if they had allowed DVR content to be controlled in a centralized way it would have created a monetization path that would have been effective for advertisers and content owners alike. -- Andrew Feinberg

Cable Executives Eye VoD

Cable executives are cooking up ways to make money on video on demand's growing popularity, attendees heard at a separate NCTA panel. These include starting an interactive, targeted advertising venture, increasing time-shifting services, and pushing electronic commerce.

Steve Burke, Comcast chief operating officer, urged cable operators and programmers to get much more creative with VoD. Industry has only "two main models" in on-demand, he said: Pay-per-view movies and TV shows briefly offered free. "We have this wonderful engine that we've created in tens of millions of homes," he said, "but the creativity to drive it into different places doesn't really seem to be there. We're using VoD in a very limited way."

Tom Rutledge, Cablevision COO, said network programmers haven't capitalized on VoD's many possibilities. Discovery CEO David Zaslav, one of two programming executives on the panel, agreed. He said interactive advertising could be a way for cable operators and programmers to counter rising Web-based competition. Zaslav also noted that, though Internet video is a growing medium, most networks haven't figured out how to "monetize" their content online.

The PVR "and the Web are both being embraced by consumers, but neither model is particularly attractive," Zaslav said. "VoD has great potential and with dynamic ad insertion could be a great business for us." He called targeted ads particularly suited to VoD because VoD viewers have chosen to watch specific programs.

Rallying support for Project Canoe -- the interactive ad standards-setting group formed this year by several large cable operators -- speakers described it as the first effort in a multistep campaign to profit from on-demand programming. Besides developing targeted, interactive commercials, Project Canoe will work on ratings and other measurement tools for VoD. "It's all about dynamic ad insertion," Time Warner Cable COO Landel Hobbs said: "The key is working on this as a sector... We've got to work together to make that cleaner and easier."

With the cable industry hiring for Project Canoe, Burke said, the consortium will announce the group's executive director June 1. "We have high hopes for it," he said.

Cable operators can use the VOD platform for "electronic sell-through" of products, additional subscription on-demand offerings, network PVR, and services like Time Warner's popular StartOver and Look Back time-shifting, Burke said. A big fan of StartOver and Look Back, Comcast is doing field trials of the services in undisclosed markets.

Hobbs said StartOver, a PVR-lite service that Time Warner has rolled out in about 10 regional divisions, has digital subscribers raving. He cited company surveys indicating that 93 percent of subscribers are satisfied with the service and 76 percent would recommend it to a friend. He said StartOver users also feel more attracted to networks enabled with the service, which lets viewers go back and watch the beginning of a program that has begun. "We are seeing nothing short of the evolution of VoD," he said. "We all wish it would go faster."

On electronic sell-through, Rutledge said Cablevision is experimenting with a DVDs-on-demand service called Popcorn. The service lets subscribers buy movies electronically and immediately watch them on TV while they wait for the DVDs to arrive.

"It's not priced properly, and the inventory is too limited for it to be a huge success at the moment," Rutledge said. Nor does it use electronic delivery. But even in this primitive form, he said, the service shows promise. "The big difference between us and the Internet is that we know who our customers are," he said. "We can ship things to them."

111 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
COMMUNICATIONS DAILY

May 20, 2008 Tuesday

LENGTH: 705 words**HEADLINE:** Election Year Means Talk, Little Action, Hill Staffers Say**BODY:**

NEW ORLEANS -- Expressions of concern were coupled with predictions that there would be little action on telecom legislation in this election year, said a panel of Hill staffers at the NCTA convention. A discussion about network neutrality legislation produced few fireworks, with House Commerce staffers from both sides agreeing that market solutions would be the first option rather than legislating a regulatory framework. Amy Levine, counsel to Chairman John Dingell, D-Mich., said that "where we go from here depends a lot on what happens out in the marketplace."

Net neutrality legislation is even less likely to move through the committee in an election year, Levine said. But another high-profile incident like the Comcast-BitTorrent controversy could "increase the impetus for Hill action," she said, adding that industry initiatives to deal with the problem such as the Comcast-BitTorrent deal and recent industry P4P Working Group lessen the sense of urgency for legislative action.

P2P and network management are akin to a growing adolescent, said Commerce Committee minority counsel Neil Fried. "In terms of where the industry developments are, we're still in our teenage years... and the last thing we want to do is stunt that growth." Fried praised network managers' attempts to cooperate with software developers. He also lauded improvements in P2P technology and network management techniques as "the market process we want," but was skeptical of a legislative solution.

Levine and Fried agreed that transparency and disclosure were key points of any network management regime. Levine said there had always been an exception in network neutrality principles for "legitimate, non-discriminatory network management" to protect customer quality of service. Fried said "the biggest issue is disclosure so consumers can express their frustrations" and emphasized that the market can only work "if everybody knows what's happening."

House Judiciary aide Dave Whitney pointed out that during the 109th Congress a bill sponsored by then-Chairman James Sensenbrenner, R-Wis., and then-Ranking Member Conyers had been reported out of committee but was never brought to the floor by the Republican leadership. Whitney said the bill was controversial even among Committee members, since its function had been to expand the antitrust authority of the Justice department "to pursue either unreasonable or discriminatory actions with regard to network management." He said many members, especially Republicans, prefer market-based solutions rather than government-mandated solutions.

The Senate Judiciary Committee has no network neutrality bills pending and is unlikely to take any action on the issue, according to Antitrust Counsel Seth Bloom. There is no demonstrated need for legislative action now, Bloom said. If there is misbehavior by network operators either in network management or advertising, the FTC has the authority to take appropriate action under antitrust law, he said.

A House bill (HR-3679) on video service taxes is on hold awaiting feedback from members, said House Judiciary Counsel Norberto Salinas, but no markup has been scheduled.

Universal service has accomplished its goal but needs to be updated, House Commerce Counsel Neil Fried said. Referring to a measure sponsored by Ranking Member Joe Barton, R-Texas, Fried defended Barton's view that "reverse auctions" would promote competition for telecom providers to compete to provide the best service to rural areas. Levine agreed that USF is "broken" but said a different solution, proposed by Rep. Rick Boucher, D-Va., and Lee Terry, R-Neb., would provide needed "comprehensive reform."

Re-authorization of the Satellite Home Viewer Act could prompt a reform of retransmission procedures between cable and DBS providers, Whitney said. Both the Senate and House Judiciary Committees are awaiting a report from the Copyright Office due June 30 which could provide a foundation for discussion of retransmission consent reform with the goal of "parity" between cable, DBS, and telephone companies. Levine said the other issues that could effect retransmission consent reform are carriage rights for sports programming and video on demand. -- Andrew Feinberg

113 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

May 20, 2008 Tuesday

LENGTH: 499 words**HEADLINE:** Election Year Means Talk, Little Action, Hill Staffers Say**BODY:**

NEW ORLEANS -- Expressions of concern were coupled with predictions that there would be little action on telecom legislation in this election year, said a panel of Hill staffers at the NCTA convention. A discussion about network neutrality legislation produced few fireworks, with House Commerce staffers from both sides agreeing that market solutions would be the first option rather than legislating a regulatory framework. Amy Levine, counsel to Chairman John Dingell, D-Mich., said that "where we go from here depends a lot on what happens out in the marketplace."

Net neutrality legislation is even less likely to move through the committee in an election year, Levine said. But another high-profile incident like the Comcast- BitTorrent controversy could "increase the impetus for Hill action," she said, adding that industry initiatives to deal with the problem such as the recent industry P4P Working Group lessen the sense of urgency for legislative action.

P2P and network management are akin to a growing adolescent, said Commerce Committee minority counsel Neil Fried. "In terms of where the industry developments are, we're still in our teenage years... and the last thing we want to do is stunt that growth." Fried praised network managers' attempts to cooperate with software developers. He also lauded improvements in P2P technology and network management techniques as "the market process we want," but was skeptical of a legislative solution.

Levine and Fried agreed that transparency and disclosure were key points of any network management regime. Levine said there had always been an exception in network neutrality principles for "legitimate, non-discriminatory network management" to protect customer quality of service. Fried said "the biggest issue is disclosure so consumers can express their frustrations" and emphasized that the market can only work "if everybody knows what's happening."

House Judiciary aide Dave Whitney pointed out that during the 109th Congress a bill sponsored by then-Chairman James Sensenbrenner, R-Wis., and then-Ranking Member John Conyers, D-Mich., had been reported out of committee but was never brought to the floor by the Republican leadership. Whitney said the bill was controversial even among committee members, since its function had been to expand the antitrust authority of the Justice Department "to pursue either unreasonable or discriminatory actions with regard to network management." He said many members, especially Republicans, prefer market-based solutions rather than government-mandated solutions.

The Senate Judiciary Committee has no network neutrality bills pending and is unlikely to take any action on the issue, according to Antitrust Counsel Seth Bloom. There is no demonstrated need for legislative action now, Bloom said. If there is misbehavior by network operators either in network management or advertising, the FTC has the authority to take appropriate action under antitrust law, he said. -- Andrew Feinberg

114 of 114 DOCUMENTS

Copyright 2008 Warren Communications News, Inc
All Rights Reserved
WASHINGTON INTERNET DAILY

May 16, 2008 Friday

LENGTH: 516 words**HEADLINE:** Hill E-Mail Expert Says System Needs Tune-Up**BODY:**

Congress should improve its use of e-mail for constituent communications, said Daniel Bennett, who as a Hill staffer in 1993 helped build one of the first House e-mail systems for Rep. Anna Eshoo, D-Calif. At a Center for American Progress Action Fund roundtable, Bennett said the legislative branch could do a better job of handling a rising tide of communications, now more than 300 million messages per year.

The Hill has had internal e-mail since the late 1980s. The system Bennett assembled for Eshoo made her office the first to use the medium to receive constituent communications. His methods set the standard for external e-mail systems in Congress, and, beginning with Lockheed-Martin, have been adopted by every major vendor of constituent communication management software. Bennett now advocates adoption of an extension to his original concept that he said is compatible with any system in use today.

Mail has always mattered on the Hill, Bennett said. To members, e-mail is equal in value to letters and phone calls, he said. Some Hill offices have resisted sending e-mail responses, for fear of spoofing, desire to avoid extra work and belief that people value the myth that a paper signature over an e-mail response, Bennett said.

The 2001 terror attacks, which included letters tainted by anthrax, revolutionized congressional e-mail policy, said Bennett. Not only did members make more use of their BlackBerrys, the only reliable method of communication on 9/11, but the poisoned mail and ensuing wariness caused many members to encourage constituent to use e-mail.

Staffers and advocacy groups now are locked in a battle over "astroturf" pseudo-grassroots campaigns and machine-generated "click-to-complain" messages, Bennett said. A consequence of this is that many offices disable their mail systems' ability for direct receipt of e-mail, instead forcing use of a Web form. An improved solution is needed for e-mail to remain viable for members, staff, and constituents, said Bennett.

The office of House Majority Leader Steny Hoyer, D-Md., is among the early adopters and beta testers of that system, as is Rep. Sam Farr, D-Calif. The system, now improved, could work with every Hill office, allowing staff to save hours by grouping and sorting inbound messages with more accuracy, as well as identifying bulk duplicate as spam. Constituents would benefit from the system's ability to flag unique messages, so an e-mail sent at 11:30 p.m. the night before a vote reaches a member next morning, Bennett said.

More help is on the way for beleaguered Hill staffers. Tim Hysom of the Congressional Management Foundation said his organization is about to release two reports on constituent communications. The first analyzes results of a Zogby survey of 10,000 adults polled on their contacts with Congress, a companion to a 2005 survey of Hill staff. The second, the fruit of CMF's "Communicating with Congress" project, will include recommendations for "a new concept" for communication with Congress in addition to suggestions for stakeholder groups, Hysom said. - Andrew Feinberg

***** Print Completed *****

Time of Request: Friday, February 03, 2012 20:42:31 EST

Print Number: 1828:331614956

Number of Lines: 3067

Number of Pages: 98

Send To: FEINBERG, ANDREW
CATHOLIC UNIVERSITY OF AMERICA
3600 JOHN MCCORMACK RD NE
WASHINGTON, DC 20064-0001