O'REILLY radar

Online privacy debates heat up in Washington

By Alex Howard on August 6, 2010 6:00 AM | Permalink | Comments (1) | TrackBacks (0)

The issue of electronic privacy is as hot as the weather in Washington this summer. Last week, both the House and Senate held hearings on online privacy, featuring testimony from top executives from Facebook, Apple and Google. The Washington Post published a massive investigative report on the growth of "Top Secret America" in July. And the Wall Street Journal's new series on online privacy, "What They Know," has laid bare the scope of tracking technology on the Internet. In the Information Age, our family, friends, neighbors, employers and government all have unprecedented abilities to watch one another, changing the nature of our relationships, workplaces and schools. Solving the privacy dilemma will be difficult, controversial and crucial for the nation's citizens, businesses, regulators and lawmakers.

Can privacy, social media and business get along? The balance between privacy and societal benefit will be difficult to strike, given the potential to harm civil liberties and the need to preserve the expectation of privacy described by the Fourth Amendment of the Constitution.

The risks and rewards for federal agencies that adopt Web 2.0 technology weigh government innovation and cost savings against potential security and privacy issues. The risks that social networking poses to consumers, businesses and government aren't theoretical, either, given the expansion of cybercrime and non-state actors targeting online users.

Given the context of the moment, putting online privacy in perspective will be a key component of the upcoming Gov 2.0 Summit in Washington, where Jules Polonetsky, Tim O'Reilly, John Clippinger and others will discuss privacy in the context of innovation and government. Despite the ongoing debate about Facebook privacy controls, electronic privacy reaches much further than social networking. From cellphone tracking to data brokers to cloud computing to credit bureaus to satellite imaging, our daily lives have become more scrutinized than at any point in human history.

Digital privacy matters more than ever to citizens in ever country, particularly where autocratic regimes are not constrained by the laws enacted in the United States. As privacy watchdogs like the Electronic Frontier Foundation and Electronic Privacy Information Center have highlighted, law enforcement officials have pushed privacy boundaries in the name of national security.

Privacy is not dead, though it's fair to say that some of the norms around how, where and when people are sharing information about location, purchases, reading habits or relationships have shifted for some populations. For marginalized members of society, privacy breaches can have tragic outcomes, as danah boyd has discussed in her thoughts on Facebook and radical transparency.

How might the FTC or FCC regulate online privacy?

At some point, the Federal Trade Commission (FTC) will also publish the results of the privacy roundtables it held over the past year. The FTC. currently protects consumer privacy under the the FTC Act, which directs the commission to "guard against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information." The FTC also has purview over regulating financial privacy under the Gramm-Leach-Bliley Act, consumer privacy under the Fair Credit Reporting Act and the Children's Online Privacy Protection Act. The Department of Health and Human Services enforces healthcare privacy breaches under HIPAA and now the HITECH Act.

Specific new guidance for the FTC from Congress on electronic privacy, however, has yet to emerge. One direction for legislation comes from the Digital Due Process Coalition, which advocates for an update to the Electronic Communications Privacy Act, given the considerable changes to mobile, location, cloud computing, webmail and social networking technology since it was enacted in 1986.

In his testimony on online privacy before the Senate Commerce Committee last week, FTC Chairman Jon Leibowitz acknowledged the online advertising industry's principles for self-regulation, including "results that were encouraging." That said, he observed that "if we don't see more progress, we probably will see more focus on prescriptive rules in the next Congress."

Leibowitz noted three principles for online privacy that had emerged from the roundtables:

1. Privacy baked in from the beginning, or "privacy by design
2. Simplified controls, including the potential for a "do not track" mechanism in a Web browser
3. More transparency about how private information would be used

In general, the use of private data should be opt-in, not opt-out, said Leibowitz, with clear notice. "Most of the cases that we've brought involve instances where disclosures or use of information was in fine print or designed to be where consumers can't find it," he said. "Good companies want to make these things clear."

FCC Chairman Genachowski, who testified with the FTC Chairman, noted that "the privacy issues discussed here are not only a fundamental moral issue. To get the economic effects of broadband, people need to be confident that the Internet is a trustworthy place." With adequate information and real choice, Genachowski said that there was an increasing chance that the market will work.

"With technology changing as rapidly as it does, the lesson should be to pull out core principles and strategies that will work, regardless of how technology evolves," he said.

Whatever the FTC or FCC do with regards to regulating online privacy, however, is likely to ultimately rely upon Congressional action. The financial regulatory reform bill signed into law by President Obama did not ultimately grant the FTC increased rulemaking authority to regulate online privacy autonomously.

Online privacy hearings in Congress

As security technologist Bruce Schneier has argued, privacy and control are closely intermingled. "If we believe privacy is a social good, something necessary for democracy, liberty and human dignity, then we can't rely on market forces to maintain it." wrote Schneier. "Broad legislation protecting personal privacy by giving people control over their personal data is the only solution."

The nature of that legislation will be on the legislative agenda of Congress this fall after the August recess. Online privacy bills were introduced in the House this year, with varying reactions from industry and privacy advocates.

Rep. Rush's privacy bill (H.R.5777), has received strong pushback from tech firms, due to its potential restrictions on firms that store personal data. Rep. Boucher's online privacy bill garnered criticism from both industry and advocacy groups.

Privacy and security concerns were highlighted at a House Judiciary subcommittee hearing on social networking last week. At the hearing, the FBI's Gordon Snow described a rising tide of online fraud, identity theft and phishing schemes over Facebook and other networks, where cybercriminals compromised other accounts due to higher levels of trust from familiar senders.

"Symantec created more malware signatures in the last 15 months than in the past 18 years combined," said Joe Pasqua, the security software company's head of research. A representative of the Secret Service said that the use of social engineering had increased as more sophisticated cybercriminals used multi-faceted attacks to trick users into divulging sensitive personal information or account details. The 2010 Verizon Data Breach Investigations Report, released on the day of the hearing, was a joint effort with the Secret Service.

"Facebook and other social networks have the power to enrich people's lives in ways that were unimaginable before," said Facebook Chief Security Officer Joe Sullivan, testifying in the hearing. Sullivan said that Facebook was the first major service that required people to build profiles with their real names, "an important choice that allowed people to become more connected and made the service safer." Sullivan, a former federal prosecutor who specialized in high tech crime in Silicon Valley, asked lawmakers for help with improving cyberliteracy with teachers and students. He also requested broader access to hashes for known images of exploited children that Facebook could run against its database of more than 50 billion pictures, the largest photography collection online.

Sullivan was challenged by EPIC founder Marc Rotenberg, who urged Congress to strengthen privacy laws for Facebook users. Rotenberg said EPIC filed an FTC complaint because of changes in Facebook's privacy settings last December that created exposure that users couldn't control. It was an "unprecedented event in the history of the Internet," said Sullivan, where Facebook "wouldn't let you use the service gain until you go through those pages."

The shift presented users with a mandatory wizard that, as Nick Bilton reported in his story on Facebook privacy, required users to click through more than 50 buttons to fully opt-out."What Facebook needs is not a Geek Squad but a Granny Squad," said Rep. Zoe Lofgren (D-CA) on the need for simpler privacy controls.

Sullivan emphasized the contextual privacy controls that allow users to specify who an update is shared with on Facebook. "We want people to make decisions for themselves," he said. "Personally, I choose to share quite a bit, and put different levels of visibility on different types of information."

That personal choice is at the crux of any statutory solution: if people choose to share information freely online or make an error, neither the government nor tech companies can help. Where the code created by technology providers matters, as Rep. Lofgren observed, is in giving people "the opportunity to have their rights respected."

Perhaps the most meaningful right is whether user information, behaviors or connections are shared publicly or privately by default. As danah boyd said in her keynote address to the 2010 SXSW Festival, "defaults matter. That's even more so for teenagers and children, whose safety was a recurrent concern at every hearing on online privacy I've attended in Washington. Sullivan noted that Facebook's default settings are different for people under 18, "in terms of what we allow them to do or the type of information made visible to them."

Questions about child predators were pervasive at the Senate hearing on online privacy, where Senator Klobuchar (D-MN) focused much of her questioning on the issue and Senator Rockefeller (D-WV) repeatedly voiced his concerns on that count.

"Good parenting is right at the center of protecting children online," said the Cato Institute's Jim Harper in reply. "You're not going to come up with a magical tech solution."

Klobuchar also questioned Google's Alma Whitten about where Google's users learn about its privacy dashboard. Whitten, whose testimony is embedded below, said that she was "adamant when we created the dashboard that it not be strictly a privacy tool. It needed to be useful."

Senator Kerry (D-MA) focused his questioning upon Facebook privacy controls and deep packet inspection. "It's fair to say there's a lot of confusion," he said, "with a lot of anxiety in the public at large over what power they have over information. It's not just a commercial component. Information collected might be incorrect or out of context, or might be correct and last longer in the market than they might like to."

AT&T's representative did publicly attest to using deep packet inspection in their network "for trying to find malware, spyware or purposes of network security." In fact, the federal government itself is using deep packet inspection as part of its cybersecurity initiative as part of its EINSTEIN surveillance program. As Harper observed in his written testimony, "if the federal government is going to work on privacy protection, it should start by getting its own privacy house in order."

Senator McCaskill (D-MO), by contrast, was concerned about consumers' understanding of their electronic privacy when they printed online coupons to be scanned for offline deals. While McCaskill's questions to Google's representative on that count were misplaced, the issue of whether citizens truly understand how much information is being gathered about their online activity is legitimate and goes to the crux of whether the traditional "notice and consent" model of privacy protections in the terms of service for platforms and software will be viable in the future.

"National surveys at Annenburg show that large numbers of Americans don't understand how database marketing works," testified Professor Joseph Turow of the University of Pennsylvania.

That prompted Senator Rockefeller to voice a philosophical question, as to whether "we are dividing ourselves into two classes of people," where some who understand the complexities of online privacy are protected and other who cannot paying a price that they cannot fully understand.

"I used to believe that could be solved by education," said Turow. "I no longer believe that. It's much too complex. Privacy policy is a scavenger hunt, where links send you into other links to affiliates." Turow expressed his concern where many people are unaware of how the information they consume has been customized to their stored data. "We're going to have a situation where people receive views of the world based upon what others know about them," he said.

The digital divide in connectivity extends, in other words, to a divide in cyberliteracy. Transparency is not enough. There is deep validity in the concerns of privacy advocates that civil liberties be preserved in the digital age, including a right to privacy that many constitutional scholars perceive in the Constitution. And yet, there are reasons to praise oversharing, as Steven B. Johnson did in Time earlier this year. There are a growing number of ways that social media helps promote better health. Anonymized community health data, can provision healthcare applications that enable citizens and cities to make better decisions. If smart grid privacy concerns can be addressed, more efficient usage could revolutionize the nation's energy infrastructure.

There may well be reasons to give up some privacy, which means that in enacting new laws and regulations to protect consumers. What happens next will be in the hands of technologists, lawmakers and the online community.

Related:

- Analysis: Three privacy initiatives from the Office of Management and Budget
- OMB updates rules for cookies and privacy on U.S. government websites
- Putting online privacy in perspective
- My contrarian stance on Facebook and privacy
- Can privacy, social media and business get along?

Identity, privacy and informed consent will be discussed at the Gov 2.0 Summit, being held Sept. 7-8 in Washington, D.C. Learn more and request an invitation.

Tags

- gov 2.0
- gov2summit
- privacy