Internet privacy controls challenge tech industry

July 26 2011, By JOELLE TESSLER , AP Technology Writer

The federal government has put Google, Microsoft, Apple and other technology companies on notice: Give consumers a way prevent advertisers from tracking their movements across the Web - or face regulation.

Yet for all its innovative know-how and entrepreneurial spirit, the technology industry has yet to agree on a simple, meaningful solution to protect consumer privacy on the Internet.

So privacy watchdogs and lawmakers are stepping up the pressure, calling for laws that would require companies to stop the digital surveillance of consumers who don't want to be tracked. They argue that effective privacy tools are long overdue from an industry that typically moves at breakneck speed.

"I want ordinary consumers to know what is being done with their personal information, and I want to give them the power to do something about it," Senate Commerce Committee Chairman John D. Rockefeller, D-W. Va., said at a recent hearing.

Washington's call to arms is a response to growing concern that invasive Internet marketing practices are eroding privacy online as every consumer move is observed, analyzed and harvested for profit.

Online publishers, advertisers and ad networks use "cookies," Web beacons and other sophisticated tracking tools to follow consumers around the Internet - monitoring what sites they visit and what links they click, what they search for and what they buy. Then they mine that information to deliver what they hope will be relevant pitches - a practice called behavioral advertising.

"Right now we have a lawful system for tracking all of our movements online," says Christopher Calabrese, legislative counsel for the American Civil Liberties Union. "And not only is it legal. It's the business model."

Calls for online privacy protections began with the Federal Trade Commission, which has challenged the industry to offer a digital tracking off switch. The FTC envisions something akin to the government's existing "Do Not Call" registry for telemarketers. Consumers who don't want to receive telemarketing calls can add their numbers to the list online or over the phone.

Companies including Microsoft and Mozilla have responded with various "Do Not Track" technologies. But an industry-wide solution is not close at hand.

That's because putting the Do Not Track concept into practice is much more complicated than simply adding phone numbers to a database. The challenge is in reaching industry consensus on what Do Not Track obligations should mean, designing standard technology tools that are easy for consumers to use and setting common rules that all Websites and advertisers will follow.

One big part of the problem is that the industry needs to find a way to let consumers halt intrusive online marketing practices without preventing tracking critical for the Internet to function. After all, Internet companies rely on tracking not just to target ads, but also to analyze website traffic patterns, store online passwords and deliver customized content like local news. Nobody wants to stop those things.

Also complicating efforts to reach broad agreement is the lucrative nature of behavioral advertising.

Industry leaders argue that many consumers like targeted ads since they deliver personalized pitches that people may want. And because these ads tend to be more effective, advertisers are willing to pay more for them, says David Hallerman, an analyst with eMarketer.

Research firm eMarketer projects U.S. spending on online behavioral advertising will hit $2.6 billion by 2014, up from $775 million in 2008.

That enables Internet companies to offer everything from online stock quotes to unlimited email storage for free, says Anne Toth, Yahoo's chief trust officer. Without sophisticated advertising technology, more websites and services could wind up behind pay walls, companies warn.

The problem, argues Jeff Chester, executive director of the Center for Digital Democracy, a privacy group, is that many consumers don't know they're being tracked. And even if they do, they have no idea what happens to their information - whether it is used to create personal profiles, merged with offline databases or sold to data brokers - and no practical way to stop the data collection.

With growing alarm in Washington, coalition of industry trade groups- called the Digital Advertising Alliance - has established a self-regulatory program that places icons inside the online ads of participating advertisers, ad networks and websites. The icon links to a site that explains online targeting, and lets consumers install an opt-out cookie if they just want standard ads.

Among the groups participating in the alliance are the Interactive Advertising Bureau and the Direct Marketing Association, as well as individual companies including Google and Yahoo.

Even so, these efforts don't go far enough for the FTC. While the agency has not endorsed any particular Do Not Track technology, it believes one promising approach could involve including a setting inside Web browsers. Now the browser companies, led by Microsoft and Mozilla, are responding with different approaches:

- Microsoft has a feature called "tracking protection" in Internet Explorer 9.0 that lets users create "black lists" of Web sites to be blocked and "white lists" of sites that are deemed acceptable. Users can set their browsers to automatically build these lists or can download existing lists.

- Mozilla has a setting in its Firefox 4 browser that sends a signal to alert websites, advertisers and ad networks if a user does not want to be tracked.

Apple is expected to include a similar feature, called a "header," in its Safari browser. Microsoft, too, recently added the feature to IE 9.0.

- Google's Chrome browser is piggybacking on the Digital Advertising Alliance by offering a plug-in that saves opt-out cookies even if other cookies are erased. One criticism of the industry program is that users lose their opt-out preferences whenever they clear their cookies.

For such tools to work, however, there must be industry consensus on what Do Not Track obligations should actually mean. And right now, there is little agreement.

Nearly everyone accepts that publishers should be able to measure traffic volumes on their own sites, for instance. But should advertisers be allowed to track how many visitors see or click on their ads?

The industry's self-regulatory program, for one, does not turn off data collection. Consumers who install an opt-out cookie no longer receive targeted ads from participating companies, but may still be tracked for non-advertising purposes. That doesn't satisfy privacy watchdogs.

Microsoft Deputy General Counsel Erich Andersen says tracking protection offers a way around this debate since it lets consumers decide what to block. But this approach worries advertisers since it can block ads altogether, even generic ads.

And anyway, with Do Not Track signals in several popular browsers, websites and advertisers need to agree on how to respond, says Jules Polonetsky, director of the Future of Privacy Forum, an industry-backed group. Otherwise, he says, Do Not Track obligations could get defined for them by browsers or government officials.

Equally important for Do Not Track to succeed, the technology must be easy to find and use. If Do Not Track tools are too confusing or involve too much effort, people won't embrace them, warns Marc Rotenberg, executive director of the Electronic Privacy Information Center. "We can't expect users to spend a lot of time reconfiguring their browsers," he says.

Privacy watchdogs are gravitating to Mozilla's approach as particularly user-friendly. But it presents a different challenge: ensuring websites, advertisers and ad networks respect user requests not to be tracked. While Microsoft's tracking protection blocks unwanted content - and requires no compliance by Websites and advertisers - a signal in a browser means nothing if it is not honored.

"Without anyone on the other end to recognize it, it's a tree falling in the woods without anyone to hear it," says Mike Zaneis, general counsel for the Interactive Advertising Bureau. Zaneis insists the Digital Advertising Alliance offers the best approach since so many Websites and advertisers are on board.

Alex Fowler, Mozilla's global privacy and public policy leader, says the browser maker is talking with many big websites, advertisers and ad networks about honoring its Do Not Track signal. And many are open to the idea. Still, so far only a handful of industry players have actually pledged to honor the signal.

And that, privacy watchdogs say, shows why the government needs to get involved.

Senator Rockefeller is sponsoring a bill that would direct the FTC to write binding, industry-wide Do Not Track rules. There are similar bills in the House and the California legislature.

The Internet marketing industry wants to head off those efforts and insists it just needs more time to establish meaningful privacy controls.

For now, FTC Chairman Jon Leibowitz is willing to give the industry a chance before calling for legislation. Even without a government mandate, he noted, it's in the industry's self-interest to make Do Not Track work. After all, Leibowitz says, "nobody wants to be on the wrong side of consumers."

Citation: Internet privacy controls challenge tech industry (2011, July 26) retrieved 18 April 2024 from https://phys.org/news/2011-07-internet-privacy-tech-industry.html