Privacy 'bill of rights' exempts government agencies

by Declan McCullagh

news analysis Two U.S. senators introduced sweeping privacy legislation today that they promise will "establish a framework to protect the personal information of all Americans."

There is, however, one feature of the bill (PDF) sponsored by senators John Kerry (D-Mass.) and John McCain (R-Ariz.) that has gone relatively unnoticed: it doesn't apply to data mining, surveillance, or any other forms of activities that governments use to collect and collate Americans' personal information.

At a press conference in Washington, D.C., McCain said the privacy bill of rights will protect the "fundamental right of American citizens, that is the right to privacy." And the first sentence of the legislation proclaims that "personal privacy is worthy of protection through appropriate legislation."

But the measure applies only to companies and some nonprofit groups, not to the federal, state, and local police agencies that have adopted high-tech surveillance technologies including cell phone tracking, GPS bugs, and requests to Internet companies for users' personal information--in many cases without obtaining a search warrant from a judge.

Senators John Kerry and John McCain at press conference announcing privacy legislation.

(Credit: U.S. Senate)

"What's a bill of rights if it doesn't provide rights against the government?" asks Jim Harper, director of information policy studies at the free-market Cato Institute.

It also doesn't apply to government agencies including the Department of Health and Human Services, the Department of Veterans Affairs, the Social Security Administration, the Census Bureau, and the IRS, which collect vast amounts of data on American citizens.

The Department of Veterans Affairs suffered a massive security breach in 2006 when an unencrypted laptop with data on millions of veterans was stolen. A government report last year listed IRS security and privacy vulnerabilities. The government of Texas yesterday revealed that it disclosed the personal information of 3.5 million citizens, including Social Security numbers. Even the Census Bureau has, in the past, shared information with law enforcement from its supposedly confidential files.

Another feature missing from Kerry and McCain's bill of rights: a strict requirement that would force federal agencies to notify American citizens in the event of a data breach.

In 2007, the Bush White House asked agencies (PDF) to develop breach notification rules. But there are no civil or criminal penalties if violated, and agencies are allowed to make their own decisions as to whether a breach has generated sufficient "harm" to warrant notification--a self-policing measure that gives them a strong incentive to downplay any potential ill effects.

Making the governmental exemption more pointed is the fact that the senators' press conference comes as the Obama Justice Department is lobbying for broader surveillance powers and trying to head off pro-privacy reforms.

In January, the Justice Department announced that investigations "are being frustrated" because no law currently exists to force Internet providers to keep track of what their customers are doing. A month later, the FBI outlined its push for expanded Internet wiretapping authority.

Last week, the Justice Department said it opposed proposals--backed by AT&T, Google, Microsoft, eBay, the American Civil Liberties Union, and Americans for Tax Reform--to protect Americans' privacy by requiring a search warrant to access online files and track Americans' locations. Then, on Friday, the Justice Department renewed its opposition to being required to use a search warrant to access the Twitter accounts of Wikileaks volunteers.

"Kerry and McCain are saying, 'Do as I say, not as I do,'" Harper says. "If they want to lead on the privacy issue, they'll lead by getting the federal government's house in order."

Instead, their legislation would regulate only commercial and nonprofit use of information that's personally identifiable, with exceptions for information "obtained from public records that is not merged" with other data and information "reported in public media."

The measure shares many features with similar, unsuccessful bills introduced last year: Personally identifiable information is defined as including a first and last name, a

residential mailing address, a Web cookie, an e-mail address, a telephone number, biometric data, and so on. "Sensitive" information is a subset and includes health records, religious information, or data that could lead to "economic or physical harm."

In general, personal information can only be used for a list of purposes specified in the legislation, including processing transactions, certain types of marketing, "reasonably expected" uses, and responding to police and other governmental requests. Violations would be punished by the Federal Trade Commission.

The FTC would also be given one year to set up a "safe harbor" program, which would be administered by approved non-governmental organizations. Companies that participate in the safe harbor, as long as it includes similar data use restrictions, would be "exempt" from the more restrictive aspects of the bill.

Read more: http://news.cnet.com/8301-31921_3-20053367-281.html#ixzz1JPZ2CDu6