January 24, 2011 2:24 PM PST

# GOP pushing for ISPs to record user data

by Declan McCullagh

The House Republicans' first major technology initiative is about to be unveiled: a push to force Internet companies to keep track of what their users are doing.

A House panel chaired by Rep. F. James Sensenbrenner of Wisconsin is scheduled to hold a hearing tomorrow morning to discuss forcing Internet providers, and perhaps Web companies as well, to store records of their users' activities for later review by police.

One focus will be on reviving a dormant proposal for data retention that would require companies to store Internet Protocol (IP) addresses for two years, CNET has learned.

Tomorrow's data retention hearing is juxtaposed against the recent trend to protect Internet users' privacy by storing *less* data. Last month, the Federal Trade Commission called for "limited retention" of user data on privacy grounds, and in the last 24 hours, both Mozilla and Google have announced do-not-track technology.

A Judiciary committee aide provided a statement this afternoon saying "the purpose of this hearing is to examine the need for retention of certain data by Internet service providers to facilitate law enforcement investigations of Internet child pornography and other Internet crimes," but declined to elaborate.

Rep. F. James Snsenbrenner of Wisconsin is scheduled to hold a hearing tomorrow morning to discuss forcing ISPs to store records of their users' activities for later review by police.

(Credit: U.S. House of Representatives)

Thanks to the GOP takeover of the House, the odds of such legislation advancing have markedly increased. The new chairman of the House Judiciary committee is Lamar Smith of Texas, who previously introduced a data retention bill. Sensenbrenner, the new head of the Subcommittee on Crime, Terrorism, and Homeland Security, had similar plans but never introduced legislation. (It's not purely a partisan issue: Rep. Diana DeGette, a Colorado Democrat, was the first to announce such a proposal.)

Police and prosecutors are the biggest backers of data retention. FBI director Robert Mueller has said that forcing companies to store those records about users would be "tremendously helpful in giving us a historic basis to make a case" in investigations, especially child porn cases. An FBI attorney said last year that Mueller supports storing

Internet users' "origin and destination information," meaning logs of which Web sites are visited.

And the International Association of Chiefs of Police, which will be sending a representative to tomorrow's hearing, previously adopted a resolution (PDF) calling for a "uniform data retention mandate" for "customer subscriber information and source and destination information." The group said today in an e-mail exchange that it still supports that resolution.

Jim Harper, director of information policy studies at the free-market Cato Institute, says the push for legislation is an example of pro-regulatory Republicans. "Republicans were put in power to limit the size and scope of the federal government," Harper said. "And they're working to grow the federal government, increase its intrusiveness, and I fail to see where the Fourth Amendment permits the government to require dragnet surveillance of Internet users."

Representing the Obama administration at tomorrow's hearing will be Jason Weinstein, deputy assistant attorney general for the Justice Department's criminal division, who has previously testified (PDF) on intellectual property infringement and was chief of the violent crime section of the U.S. Attorney's office in Baltimore.

For now, the scope of any mandatory data retention law remains hazy. It could mean forcing companies to store data for two years about what Internet addresses are assigned to which customers (Comcast said in 2006 that it would be retaining those records for six months).

Or it could be more intrusive, sweeping in online service providers, and involve keeping track of e-mail and instant-messaging correspondence and what Web pages users visit. Some Democratic politicians have previously called for data retention laws to extend to domain name registries and Web hosting companies and even social-networking sites. The police chiefs' proposal talks about storing information about "destinations" that Internet users visit.

AOL said today that "we are waiting to see the proposed legislation to understand what data needs to be retained and for what time period."

These concepts are not exactly new. In June 2005, CNET was the first to report that the Justice Department was quietly shopping around the idea, reversing the department's previous position that it had "serious reservations about broad mandatory data retention regimes." Despite support from the FBI and the Bush Justice Department, however, the proposals languished amid concerns about privacy, liability, cost, and scope. (Would coffee shops, for instance, be required to ID users and log their activities?)

**Retention vs. preservation**

At the moment, ISPs typically discard any log file that's no longer required for business

reasons such as network monitoring, fraud prevention, or billing disputes. Companies do, however, alter that general rule when contacted by police performing an investigation--a practice called data preservation.

A 1996 federal law called the Electronic Communication Transactional Records Act regulates data preservation. It requires Internet providers to retain any "record" in their possession for 90 days "upon the request of a governmental entity."

Because Internet addresses remain a relatively scarce commodity, ISPs tend to allocate them to customers from a pool based on whether a computer is in use at the time. (Two standard techniques used are the Dynamic Host Configuration Protocol and Point-to-Point Protocol over Ethernet.)

In addition, Internet providers are required by another federal law to report child pornography sightings to the National Center for Missing and Exploited Children, which is in turn charged with forwarding that report to the appropriate police agency.

When adopting its data retention rules, the European Parliament required that communications providers in its 25 member countries--several of which had enacted their own data retention laws already--retain customer data for a minimum of six months and a maximum of two years.

The Europe-wide requirement applies to a wide variety of "traffic" and "location" data, including the identities of the customers' correspondents; the date, time, and duration of phone calls, voice over Internet Protocol calls or e-mail messages; and the location of the device used for the communications. The "content" of the communications is not supposed to be retained.

But last March, a German court declared the national data retention law to be unconstitutional.