DOJ seeks mandatory data retention requirement for ISPs

By Jaikumar Vijayan, Framingham | Wednesday, 26 January, 2011

The U.S. Department of Justice and an organization representing police chiefs from around the country renewed calls on Tuesday for legislation mandating Internet Service Providers (ISP) to retain certain customer usage data for up to two years.

The calls, which are stoking long standing privacy fears, were made at a hearing convened on Tuesday by a House subcommittee that is chaired by Rep. James Sensenbrenner, a Republican congressman from Wisconsin. Four years ago, Sensenbrenner proposed, and then quickly withdrew, legislation calling for mandatory data retention for ISPs.

In prepared testimony for today's hearing, Jason Weinstein, deputy assistant attorney general at the Justice Department, said that data retention was crucial to fighting Internet crimes (PDF document) , especially online child pornography.

Current policies that only require ISPs to preserve usage data at the specific request of law enforcement authorities are just not sufficient, Weinstein said. Increasingly, law enforcement authorities are coming up empty-handed in their efforts to go after online predators and other criminals because of the unavailability of data relating to their online activities, Weinstein said.

"There is no doubt among public safety officials that the gaps between providers' retention policies and law enforcement agencies' needs, can be extremely harmful to the agencies' investigations," he said in written testimony.

In many cases, ISPs are already collecting and maintaining "non-content" records about who is using their services and how for business reasons, and for handling issues such as customer disputes, Weinstein said. Those same records can be extremely useful in criminal investigations too, he said.

However, ISPs have widely varying policies for storing such data, with some deleting it in a manner of days and others retaining it for months, he said. By making it compulsory for them to store usage data for specific lengths of time, law enforcement authorities are assured of getting access to the data when they need it, he said.

In his testimony, Weinstein admitted that a data retention policy on the industry raised valid privacy concerns. However, such concerns need to be addressed and balanced against the need for law enforcement to have access to the data, he said. "Denying law enforcement that evidence prevents law enforcement from identifying those who victimize others online," Weinstein said.

John Douglas, chief of police in Overland Park, Kansas and a representative of the International Association of Chiefs of Police, echoed similar concerns (PDF) .

"Clearly, preserving digital evidence is crucial in any modern-day criminal

investigation," Douglas said in his prepared testimony for the House subcommittee. On occasion, law enforcement has been able to use existing legal processes to get ISPs to preserve data in connection with specific investigations, he said.

However, because of widely varying data retention policies, sometimes law enforcement requests for protecting data are made too late. "There are cases where we are not able to work quickly enough -- mostly because a 'lead' is discovered after the logs have expired or we are unaware of the specific service provider's protocols concerning data retention time periods," Douglas said.

Calls for a new data retention policy are not new. In the past, numerous others, including FBI director Robert Mueller and former attorney general Alberto Gonzalez, have also urged Congress to consider similar legislation.

It's unclear yet if Tuesday's House hearing is a sign that a data retention bill is imminent, said John Morris, the general counsel for the Center for Democracy and Technology, a Washington D.C.-based think-tank.

Also unclear is whether it is only ISPs that will be required to retain data, or whether services such as e-mail providers might be included, said Morris, who also testified at the hearing. A similar question mark hangs over what data exactly it is that ISPs and potentially others will be required to retain, Morris said.

In the best-case scenario, a data retention bill will only require ISPs to track and store Internet Protocol (IP) address allocation data to help law enforcement better link Internet use to specific users, he said. In the worst-case scenario, it could require ISPs and all sorts of online service providers to store and track everything from IP addresses to source data involving e-mail, instant messaging (IM), social media interactions and Web sites visited, he said.

Regardless of the scope, mandatory data retention laws raise important privacy and free speech concerns, he said. "In the privacy realm, the bottom line is that law enforcement is talking about having a massive amount of information on 230 million presumably innocent Americans using the Internet, being tracked and retained," he said.

The notion that an Internet user's every move could potentially be recorded will have a chilling effect on free speech and anonymous speech, he said. It will also have an impact on how freely individuals use the Internet to search for certain kinds of information, such as that related to specific diseases for instance, Morris said.

Any kind of mandatory data retention requirement will be akin to "dragnet surveillance by the government," said Jim Harper, director of information policy studies at the Cato Institute, a Washington D.C.-based public policy research organization with libertarian leanings. "It will only look like it is not because it is will be a regulatory requirement for businesses and not wiretapping ," he said.

"The fact that people's activity on the Internet is recorded at some point [by ISPs] does not mean the government needs to have access to that data," he said.

Jaikumar Vijayan covers data security and privacy issues, financial services security and e-voting for Computerworld. Follow Jaikumar on Twitter at @jaivijayan or subscribe to Jaikumar's RSS feed . His e-mail address is

jvijayan@computerworld.com .