Obama's Surveillance Power Grab

The Obama administration wants to "clarify" FBI power to get online records without warrants -- and vastly expand it.

JULIAN SANCHEZ | *July 29, 2010* | web only

FBI Director Robert Mueller during a news conference on the gathering of personal information. (AP Photo/Susan Walsh)

They're calling it a tweak -- a "technical clarification" -- but make no mistake: The Obama administration and the FBI's **demand** that Congress approve a huge expansion of their authority to obtain the sensitive Internet records of American citizens without a judge's approval is a brazen attack on civil liberties.

At issue is the scope of the Federal Bureau of Investigation's power to obtain information from "electronic communications service providers" using National Security Letters (NLS), which compel private companies to allow government access to communication records without a court order. The administration wants to add four words -- "electronic communication transactional records" -- to **Section 2709 of the Electronic Communications Privacy Act**, which spells out the types of communications data that can be obtained with an NSL. Yet those four little words would make a huge difference, potentially allowing investigators to draw detailed road maps of the online activity of citizens not even suspected of any connection to terrorism.

In their original form, NSLs were extremely narrow tools designed to allow federal investigators to obtain very basic telephone records (name, address, length of service, calls placed and received) that could be linked by "specific and articulable facts" to persons suspected of being terrorists or foreign spies. In 1993, Congress amended the statute to clarify that NSLs could be issued to electronic information service providers as well as traditional phone companies. But wary of the potential for misuse of what the House Judiciary Committee called this "extraordinary device" in a world of rapidly changing technology, Congress placed tight limits on the types of records that could be obtained, making clear that "new applications" of NSLs would be "disfavored."

The administration is **presenting** this change as a mere clarification meant to resolve legal ambiguity -- as though Congress had simply misplaced a semicolon. Yet the Bush-era Office of Legal Counsel already rejected that argument in a **2008 opinion**, concluding that the FBI had for years misread the "straightforward" language of the statute. And clarity is certainly needed, as it is hard to know just what falls under "categories of information parallel to subscriber information and toll billing records." The standard reference for lawyers in this sphere, David Kris' *National Security Investigations and Prosecutions*, simply notes that the scope of NSLs as applied to online activity is unclear. Even the Justice Department seems uncertain. In a 2001 response to congressional inquiries about the effect of the newly enacted PATRIOT Act, DOJ **told** Congress that "reasonable minds may differ" as to where the line should be drawn between addressing information equivalent to toll billing records and "content" requiring a search warrant.

Congress would be wise to specify in greater detail just what are the online equivalents of "toll billing records." But a blanket power to demand "transactional information" without a court order would plainly expose a vast range of far more detailed and sensitive information than those old toll records ever provided.

Consider that the definition of "electronic communications service providers" doesn't just include ISPs and phone companies like Verizon or Comcast. It covers a huge range of online services, from search engines and Webmail hosts like Google, to social-networking and dating sites like Facebook and Match.com to news and activism sites like RedState and Daily Kos to online vendors like Amazon and Ebay, and possibly even cafes like Starbucks that provide WiFi access to customers. And "transactional records" **potentially** covers a far broader range of data than logs of e-mail addresses or websites visited, arguably extending to highly granular records of the data packets sent and received by individual users.

As the Electronic Frontier Foundation **has argued**, such broad authority would not only raise enormous privacy concerns but have profound implications for First Amendment speech and association interests. Consider, for instance, the implications of a **request for logs** revealing every visitor to a political site such as Indymedia. The constitutionally protected right to anonymous speech would be gutted for all but the most technically savvy users if chat-forum participants and blog authors could be identified at the discretion of the FBI, without the involvement of a judge.

The right of "expressive association," which **a unanimous Supreme Court** similarly found to enjoy constitutional protection, would be equally imperiled. Though, the Court previously held that the government could not force politically controversial groups like the NAACP to reveal their membership rosters without judicial process. But as legal scholar Katherine Strandburg **has argued**, data-mining technology now holds out the temptation that just such patterns of "expressive association" can be revealed by sophisticated analysis of communications patterns and social-network ties -- and perhaps even patterns of physical movement, as could be inferred from records of location-sensitive mobile devices. And when the goal is to detect the patterns of previously unidentified terrorists, such analysis requires vacuuming up the records of huge numbers of innocent persons, more or less by definition.

Moreover, the distinction between "content" and merely "transactional" information is not nearly as sharp as might be supposed. Certain communications protocols, for instance, transmit each keystroke a user makes in real time as a separate data "packet." Given the known regularities of the English language, standard keyboards, and human hands, it is **theoretically possible** to infer the content of a communication from a sufficiently precise record of packet transmission timing. While such an attack would probably be infeasible given current technologies and record-keeping practices, the legal change proposed by the FBI would not be limited to present technologies or practices.

More practically, consider records of keyword-sensitive targeted advertising delivered to users of Webmail services like Gmail, which could indirectly hint at the contents of the e-mail that triggered a specific ad. Or again, consider downloaded movies. Under the **Video Privacy Protection Act of 1988**, records of a customer's video-rental history are private and protected by law. But even if subscriber viewing histories using services like iTunes or Netflix were considered out of bounds, that history could be reconstructed from transaction logs showing the precise size of a user download. The examples are hypothetical -- what matters is the more general point: An abstract distinction between metadata and "content" gives us no way of predicting the extent of highly intimate information that might be extracted as technology changes and the analytic tools of investigators become more sophisticated.

We increasingly live online. We flirt, shop, read, speak out, and organize in a virtual space where nearly every action leaves a digital trace -- and where those breadcrumb bits often track us through the physical world as well. If the Obama administration gets its way, an agency that has already proved itself utterly unable to respect the limits of its authority will have discretion to map our digital lives in potentially astonishing detail, with no judge looking over their shoulders. That the administration and the FBI would seek such power under the guise of a "technical clarification" is proof enough that they cannot be trusted with it.

★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★★

Julian Sanchez is a writer based in Washington, D.C., and a research fellow at the Cato Institute.