WIRED

Court Says Tracking Web Histories Can Violate Wiretap Act

Andy Greenberg

November 10, 2015

Federal courts have long given the government leeway to surveil and collect so-called "non-content" data—records of the senders and recipients of calls and emails, for instance, rather than contents of those communications. But an unlikely case involving Google may mean the government will be required to get a warrant before it sucks up one type of that metadata: the detailed history of an individual's web browsing.

On Tuesday the third circuit court of appeals issued a ruling in a long-running class action lawsuit against Google and two media firms, who are all accused of circumventing cookie-blocking technologies in browsers to track users' web histories. In the ruling, the appeals court agreed with a lower court, which dismissed the plaintiffs' claims that Google and the other defendants had violated laws like the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act by collecting users' web browsing information. (Though the ruling does reverse the dismissal of a different claim that the defendants violated the California constitution, which will now proceed in the lawsuit.) But despite those decisions and perhaps more importantly, the court was careful to make another point: That merely tracking the URLs someone visits can constitute collecting the contents of their communications, and that doing so without a warrant can violate the Wiretap Act. And that's an opinion that will apply not just to Google, but to the Justice Department.

"This is a pretty big deal for law enforcement," says Jonathan Mayer, a Stanford fellow in computer science and law whose research into Google's circumvention of cookie-blocking technology helped to spark the class action as well as the search giant's $17 million settlement with 37 states on the issue. "The punchline is that if the FBI or any law enforcement agency wants to to look at your web history, they'll have to get a warrant for a wiretap order," which

requires proving a tougher standard of "probable cause" to a judge than would be necessary for collecting mere metadata.

In their ruling, the panel of three appellate judges found that Google and its co-defendants hadn't violated the Wiretap Act because they were a "party" to the communications rather than a third-party eavesdropper—the users were visiting their websites when the cookies were installed. But the judges took special pains to make clear that the defendants hadn't been let off because their cookie-blocking circumvention technique was only collecting metadata from users, rather than the content of their communications. The URLs that a web user visits, the court explained, can in fact qualify as content and thus require a warrant to surveil. "If an address, phone number, or URL is instead part of the substantive information conveyed to the recipient, then by definition it is 'content,'" the ruling reads. "[Due to] the information revealed by highly detailed URLs…we are persuaded that—at a minimum—some queried URLs qualify as content."

A visit to "webmd.com," for instance, might count as metadata, as Cato Institute senior fellow Julian Sanchez explains. But a visit to "www.webmd.com/family-pregnancy" clearly reveals something about the visitor's communications with WebMD, not just the fact of the visit. "It's not a hard call," says Sanchez. "The specific URL I visit at nytimes.com or cato.org or webmd.com tells you very specifically what the meaning or purport of my communications are."

In fact, Sanchez says that the Department of Justice already officially states that it seeks a warrant when it collects URLs from a suspect's web history. The judges in the Google case also cite a formerly secret Foreign Intelligence Surveillance court ruling that also found that URLs could count as content as well as metadata. But Sanchez argues that the new, more public ruling nonetheless helps to cement that precedent and prevent the DOJ from changing its policy. The ruling could also stop lower-level law enforcement from warrantlessly collecting web history.

The ruling could also be a first step toward erasing the metadata/content distinction for other types of communications, too. Sanchez argues that email can also blur that line, since an internet service provider might only know the mail server an email is being sent to, and the specific address of the recipient might be considered the "contents" of that message. "It's not as though there's a clean divide between the envelope and the stuff inside," Sanchez says. "It's more like an onion with different layers of metadata."