

What Do the Twitter 'Subpoenas' Mean?

by [Jim Dempsey](#) [1]
January 12, 2011

News that the Justice Department had obtained a court order directing that Twitter turn over records relating to several individuals associated with Wikileaks has raised once again questions about the standards for government access to the ocean of data generated about our activities in the digital age.

On the one hand, the Twitter story really should not come as a surprise: It is known that the government is conducting a criminal investigation of the disclosure of classified information to WikiLeaks and is trying to determine if there is any liability on the part of WikiLeaks staff or volunteers. At this stage, investigators are likely casting a broad net. WikiLeaks head Julian Assange and others working with WikiLeaks have used Twitter. While Tweets are public, Twitter logs may have IP addresses and other information that could lead to other service providers and more revealing information.

As a matter of evidence and constitutional law, there is very little if any information that is off-limits to the government, especially when that information can be obtained from someone other than the record subject.

And the Internet is a remarkable repository for information about our daily lives, held by the service providers upon whom we depend as a matter of convenience and even necessity. Last week, when I was on KQED's Forum program talking about digital search and seizure issues, one of the other guests, Matt Parrella, a federal prosecutor and computer crime expert, explained how the government views the Internet:

"From law enforcement's perspective, entities like Google, Yahoo, Hotmail, other large Internet Service Providers, have become repositories for evidence on a scale that has never existed before. ... There is, simply put, more evidence and its more important and its nowhere else than these places."

But while it should be no surprise that investigators in a transnational, Internet-focused case are going to one of these "repositories of evidence" - and are certainly going to others with even richer stores of data - the Twitter case does focus attention on the legal standards regulating the government's access to information.

Outpaced by Technology

As we have [noted in previous posts](#) [2] the main federal statute on Internet surveillance, the Electronic Communications Privacy Act (ECPA), is outdated. When it was adopted in 1986, ECPA was the right law for its time, but technology has advanced at a rapid pace and the legal protections have failed to keep pace.

ECPA sets up a sliding scale of authorities the government can use to compel service providers to disclose information. At the lowest level, the government can use a subpoena, issued by a prosecutor without approval of a judge. Further up the ladder, the government can obtain an order from a judge, where the government provides "specific and articulable facts showing . . . reasonable grounds to believe that the ... information sought [is] relevant and material to an ongoing criminal investigation." These intermediate orders are known as "2703(d) orders," since they are issued under section 2703(d) of ECPA as codified in Title 18 of the United States Code. And, at the top of the scale, for certain information, the government must obtain a search warrant, issued by a judge based on a showing of probable cause to believe that a crime has been committed and that evidence relevant to the crime is likely to be obtained by the disclosure. Probable cause is the standard specified in the Constitution for issuance of warrants to intrude on our "persons, houses, papers, and effects."

A sliding scale makes sense. The trouble is that ECPA applies it in an inconsistent and probably unconstitutional way. Notably, the most sensitive information, the content of private communications, is sometimes available to the government with the lowest form of process, the prosecutor's subpoena. In addition, the US Justice Department claims that another very sensitive form of information, cell phone tracking data, is available with a 2703(d) order, without the probable cause finding.

CDT has helped organize a [coalition of Internet companies](#) [3], think tanks and public interest groups from across the political spectrum arguing that ECPA should be updated, to extend the warrant requirement to all private communications and to cell phone tracking data. The warrant is quite a workable standard - law enforcement is quite effective operating under it in the real world.

And the courts are beginning to recognize that ECPA does not provide the protection required by the Constitution: Last month, a [federal appeals court held](#) [4], under the Fourth Amendment, that all email should be protected by the warrant requirement and a federal magistrate held that the Constitution require a warrant for all cell phone tracking. (More on that case in a later post.)

Back to Twitter: Despite some press reports, the government did not use a prosecutor's subpoena. As Orin Kerr [explained here](#) [5] and [in this radio segment](#) [6], the government obtained a court order for the WikiLeaks data, issued under section 2703(d). Although Internet logs can be very revealing, the Digital Due Process recommendations do not call for changes to section 2703(d).

But the bigger point of the Twitter story is this: Given our increased - and almost unavoidable - reliance on the Internet in our personal and professional lives, ECPA in its current form simply does not offer sufficient protection. Both the courts and Congress must respond, striking a better balance between government power and individual privacy. Those who want to Tweet their lives can continue to make that choice, but those who want privacy in their personal communications and whereabouts should enjoy the same privacy digitally that the Framers of our Constitution wanted for their "papers."

- [Twitter](#)
- [Security & Surveillance](#)
- [ECPA](#)
- [DOJ](#)
- [digital due process](#)

The content © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/blogs/jim-dempsey/what-do-twitter-subpoenas-mean>

Links:

[1] <https://cdt.org/personnel/jim-dempsey>

[2] <http://www.cdt.org/blogs/harley-geiger/updating-privacy-protections-21st-century-communications>

[3] <http://www.digitaldueprocess.org>

[4] <http://www.cdt.org/blogs/joshua-gruenspecht/courts-boldly-go-fourth-rulings-validate-digital-due-process>

[5] <http://volokh.com/2011/01/11/2703d-orders-in-the-news-no-really/>

[6] <http://marketplace.publicradio.org/display/web/2011/01/11/tech-report-the-justice-department-wants-information-from-twitter/>