JUST SECURITY
A FORUM ON LAW, RIGHTS, AND U.S. NATIONAL SECURITY

Reading Jack Goldsmith's STELLARWIND Memo (Part II)

By Julian Sanchez

Tuesday, September 16, 2014

Last week, I tried to read between the lines of Jack Goldsmith's 2004 memorandum on the STELLARWIND surveillance program to explain why the bulk collection of Internet metadata had proven so controversial with Justice Department Attorneys. As I noted in that post, we can be reasonably certain that the perceived problem was statutory rather than constitutional, because Goldsmith cites *Smith v. Maryland* in support of the (seemingly categorical) proposition that collection of metadata does not implicate the Fourth Amendment at all. This is a distressingly common gloss on *Smith*, and one can point to isolated sentences from the opinion—as Goldsmith does—that seem to support that reading when taken out of context. But *Smith* simply does not say anything so sweeping, and for reasons I laid out in detail in one of my very first *Just Security* posts, the holding in *Smith* cannot reasonably be stretched to cover the acquisition of e-mail metadata *from Internet backbone providers*, which is where where NSA appears to have been collecting it under STELLARWIND.

For the uninitiated: *Smith* established that the acquisition of telephonic metadata from a phone company, which routinely preserved the same information in its ordinary business records, did not constitute a Fourth Amendment search of the customer's person, papers, or effects. That is not remotely the same thing as a holding that all forms of metadata fall beyond the protection of the Fourth Amendment, regardless of the means by which they are obtained. As a key passage Goldsmith cites from the earlier case of *United States v. Miller* explains (emphasis mine): "This court has repeatedly held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed **by him** to government authorities." Crucially, the Court is here discussing cases where information is obtained *from the very same person or entity to whom it was conveyed*. This is typically true even of the contents of communications: If I leave a voice message on my friend's answering machine, it is no Fourth Amendment search if my friend later turns the recording over to police, whether voluntarily or in response to a subpoena. Indeed, even if the government obtains my message by an illegal search of my friend's home, in clear violation of *his* Fourth Amendment rights, I may not have standing to invoke *my* Fourth Amendment rights to exclude the recording from being introduced *against me*. It does not follow at all, however, that the Fourth Amendment offers no protection against the acquisition of the very same message via a warrantless wiretap.

The significance of *how* metadata is obtained can be obscured because, as Orin Kerr notes in his paper *Four Models of Fourth Amendment Protection*, the courts regularly employ an array of inconsistent tests and standards to determine when a Fourth Amendment search occurs. One factor courts sometimes consider is the nature or sensitivity of the information obtained: In *Smith*, the Court posits that dialing information conveyed *to* the phone company is relatively less sensitive than the contents of the conversations conveyed *through* the phone company. Whether that assumption holds true in the modern context is, at the very least, highly questionable. But even if we accept that supposition, the Court is emphatically not claiming that a particular *type* of information, metadata, is categorically beyond the protection of the Fourth Amendment. When I call an office switchboard and asked to be connected to a particular extension, my request conveys the same *type* of information we would call "metadata" if I had dialed the number directly, but it is structurally part of the content of my communication with the switchboard operator. That this type of information can often be obtained without conducting a search has no bearing on whether a wiretap to intercept my communication with the operator is a search—which, of course, it is. As Justice Scalia stressed in *Kyllo v U.S.*:

The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful.

That's important here, as I explained in that early post, because *with respect to Internet backbone providers* e-mail metadata is just another type of content, and acquiring that data off the backbone is just a plain old wiretap. While my e-mail provider, or that of my correspondent, may routinely retain e-mail metadata for ordinary business purposes, the communications provider responsible for ferrying the data between our two e-mail servers does not. It might, of course, be possible to acquire that data without performing a Fourth Amendment search by subpoenaing those e-mail providers. But a wiretap does not cease being a wiretap just because there might be ways of learning the same information without a wiretap.

One might argue that this is hairsplitting—that it makes little practical difference that NSA chose to vacuum up metadata at the backbone if the same effect could have been achieved by serving orders on e-mail providers. But Goldsmith's argument here also turns on a straightforward factual mistake:

Just like the numbers that a caller dials on a telephone, the addressing information on an e-mail is freely shared with an e-mail service provider to enable the delivery of the message. The user fully knows that he must share that information to have his mail delivered.

But this is just wrong. While most people do, of course, make use of third-party e-mail providers, it false that one *must* do so: Though it requires a moderate level of technical sophistication, in principle anyone can operate their own e-mail server on a privately owned computer, and plenty of tech savvy folks do just that. Far more commonly, corporate entities like the Cato Institute or the Associated Press or Georgetown University may act as e-mail providers for their members or employees—and in these cases the provider's relationship to the individual user is far from the arm's-length "third party" relationship of a phone company to its customers. Even if the

individual senders and recipients in these cases have waived their personal expectation of privacy in the information conveyed to the servers of the employers who maintain their accounts, those corporate entities have their own Fourth Amendment rights, and there is no third party to whom *they* have conveyed the e-mail metadata stored on their in-house servers. Rather, the metadata needed to route an e-mail message from an individual sender to an individual recipient is part of the content of a communication between (the servers of) Cato and the Associated Press—a communication conveyed *through* but not *to* the Internet backbone provider.

Goldsmith attempts to bolster his case with an analogy to postal mail, where the addressing information on the exterior of an envelope is considered exposed to the public and therefore lacking any expectation of privacy. But as the example above shows, the analogy is misleading, because these two communications technologies *don't actually function analogously*: What is "exposed" *to the backbone provider* is only an "envelope" addressed from the Cato Institute to the Associated Press—an envelope that would be "opened" upon delivery to the internal mail system of the Associated Press to expose a second envelope with more specific addressing information. The communication (or really, series of communications) between the two SMTP servers would look roughly like this:

```
CATO: MAIL FROM:<jsanchez@cato.org>
AP: 250 OK

CATO: RCPT TO:<reporter@ap.org>
AP: 250 OK

CATO: DATA
AP: 354 Start mail input; end with <CRLF>.<CRLF>
CATO: Hello, friendly journalist,
CATO: I would be delighted to share my
CATO: policy expertise with you...
CATO: <CRLF>.<CRLF>
AP: 250 OK
```

The part of this necessarily "exposed" or "conveyed to" the intermediary Internet backbone provider would be the numerical equivalents of "CATO" and "AP," whereas everything following the colon on each line is the communication between those two servers. And indeed, one reason corporations sometimes decide to maintain their own mail servers is precisely to retain exclusive possession of the contents of these inter-server communications.

If the government wishes to obtain those communication contents, whether they are interested in the addressing information being transmitted from server to server or the English message ultimately bound for a human recipient, they may subpoena the corporate sender or recipient for the appropriate business records, or obtain a conventional wiretap order to intercept the communication at the backbone. What they should not do, however, is invoke *Smith* in tandem with technically imprecise analogies to disanalogous technologies in order to pretend that a wiretap is not a wiretap.

Julian Sanchez is a research fellow at the Cato Institute and contributing editor for Reason magazine. Follow him on twitter @normative.