Slate

The Fourth Amendment Shell Game

One of Obama's NSA reforms just makes the problem worse.

By Julian Sanchez

The National Security Agency's controversial call-records dragnet has never been much use at finding terrorists, as two separate government panels have concluded, but technological change has been gradually rendering it completely irrelevant. Now, under the guise of putting an end to that program—which sweeps in the phone logs of millions of innocent Americans for later analysis—President Obama has proposed a new authority that could force private corporations to act as government spies, circumventing constitutional privacy safeguards in the process.

The current version of the NSA program is based on a Patriot Act authority that lets the government obtain records already kept by phone companies for their own business purposes. But as Reuters reported last week, the president's proposal could require carriers to *create* new records in response to the government's secret demands. To understand why this would set such a dangerous precedent, it's necessary to understand the legal theory behind the NSA program as it now exists.

If the government wants to seize your cellphone in order to learn whom you've been calling, the Fourth Amendment requires a judicial warrant, based on evidence that provides "probable cause" to believe you're up to no good. But thanks to a 1979 Supreme Court ruling, *Smith v. Maryland*, it doesn't need to meet that high standard if it collects the same information from the phone company. When you place a call, the court reasoned in *Smith*, you "knowingly expose" the number you're dialing to the phone company—and any customer who ever looked at a phone bill should be well aware that carriers keep records of those numbers, along with the times and durations of calls. In the process, the *Smith* decision argued, you waive your "reasonable expectation of privacy"—and therefore your Fourth Amendment rights. That "third party doctrine," as legal scholars have dubbed it, is why the NSA doesn't need to worry about formalities like "probable cause" or "particularized suspicion" when it vacuums up phone records in bulk.

Things have changed since the '70s, however, and increasingly phone companies aren't bothering to bill customers by individual calls—which means they may not need to keep all the detailed information NSA wants for billing purposes, at least not in a form that separates it from

information NSA is barred from collecting, like location data. Instead, they're moving to flat-rate billing that more closely resembles the model most Internet providers use, where you pay the same amount regardless of how many websites you visit or where they happen to be located. And, of course, people are moving from landlines to cellphones. As a result of all this, according to press reports, the NSA is no longer getting nearly all Americans' phone records—because in many cases, cell carriers no longer need to keep detailed records for billing purposes, any more than Comcast needs to keep logs of which YouTube videos you watch in order to send you a monthly bill.

Though Obama's plan only makes reference to telephone companies, it's already clear that most personal communications—whether text chats or voice calls—will travel over the Internet in the very near future. So it's no surprise that legislation proposed by leaders of the House intelligence committee takes the obvious next step: It applies to *all* "electronic communications" providers, a category that encompasses broadband companies like Comcast or Verizon as well as online platforms like Google and Facebook. That's a much bigger deal, because Internet services have the ability to collect a much wider array of data about their users—and also more potential to provide secure and anonymous communications by choosing *not* to collect it.

The crucial mandate there is hidden in some innocuous-sounding but ambiguous language requiring companies to "immediately provide the government with records, whether existing or created in the future, *in the format specified by the government*." (Italics mine.)

That's fine if it just means companies have to segregate the information NSA needs from the details it doesn't, or standardize their records for easy cross-referencing. But if the Reuters report is accurate, what intelligence agencies really want is the discretion to tell companies *what information* they should collect and store—at least when it comes to "suspicious" users and their friends—even if the company has no business reason to keep that data. Your broadband provider may not have any reason to track what sites you read or whom you chat with—and plenty of us would refuse to do business with one that did—but under a broad interpretation of the House language, the government can secretly force them to start doing so without a warrant. That unwisely skews corporate incentives toward broader data retention—even as privacy advocates and security experts alike urge more limited retention to protect users from data breaches.

Legal scholars have long criticized the strained logic of the *Smith* ruling, which assumes we surrender all our constitutional privacy rights in any information we share with a corporation, even under the strictest promises of confidentiality. But this new proposal stretches that logic past the point of absurdity. The only way to square such a power with the Fourth Amendment is to assume that you somehow "waive" your constitutional privacy rights in any data (other than the actual contents of a message) that flows through any corporate computer. On that logic, even if a privacy-friendly online platform pledges not to log who you're chatting with, for instance, the fact that they *could* means that information isn't private for Fourth Amendment purposes after all.

Think of it as a legal shell game: When the government orders a phone or Internet company to monitor you, the Fourth Amendment offers no protection, because that's not a *government* search. Then when the government seizes the results of that monitoring, you're

still out of luck—because now they're not taking *your* records. The courts have already embraced that shell game when it comes to banking records—but at least there, the retention mandate is an explicit part of a federal statute, not determined by secret directives from spy agencies.

As Supreme Court Justice Sonia Sotomayor has observed, the "third party doctrine" is already increasingly out of touch with ordinary people's real expectations of privacy in the Internet era. It's time to start rolling it back and restore the Fourth Amendment's teeth—not letting the government decide how much privacy we can expect. Any legislation to reform NSA's metadata program needs to make crystal clear that it only covers information that companies keep for their own reasons—not information that spy agencies want to exempt from constitutional protection.

*This article is part of Future Tense, a collaboration among Arizona State University, the New America Foundation, and **Slate**. Future Tense explores the ways emerging technologies affect society, policy, and culture. To read more, visit the Future Tense blog and the Future Tense home page. You can also follow us on Twitter.*

Julian Sanchez is a research fellow at the Cato Institute.