ASU | NEW AMERICA | SLATE

Learn more about Future Tense »

FUTURE TENSE THE CITIZEN'S GUIDE TO THE FUTURE

DEC. 13 2013 5:02 PM

How the NSA Piggy-Backs on Third-Party Trackers

By Edward Felten and Jonathan Mayer

Got cookies?

Photo by Lili Warren/AFP/Getty Images

Snooping on the Internet is tricky. The network is diffuse, global, and packed with potential targets. There's no central system for identifying or locating individuals, so it's hard to keep track of who is online and what they're up to. What's a spy agency to do?

One option is to plant a unique tag on every computer and smartphone, stamp every Internet message with the sender's tag, and then capture the tagged traffic. Perhaps in a massive database with a quirky all-caps codename. But a project of that scale can't be kept secret, and if it's done openly the public will surely object.

Luckily (for the spies) there's an easier way: free ride on the private sector, which does its own pervasive tagging and monitoring.

That's precisely what the National Security Agency has been up to, as confirmed most recently by a **front-page story** in Wednesday's *Washington Post*.Other countries' spy agencies are probably doing the same thing.

Companies track users for many reasons, such as to remember a login, to target ads, or to learn how users navigate. They usually do this by tagging each computer or smartphone with a tracking ID: a random-looking unique identifier, which is often stored in a browser cookie.

Which companies are keeping tabs on you? You probably expect to be tracked by the sites you visit and the apps you run. But these "first parties" often pull in tracking content from unrelated "third parties," most of which you probably have never heard of. ***Slate***'s home page, for example, references at least a dozen third-party trackers. When we viewed the *Post*'s story about the NSA, our browser was directed to 39 third-party trackers, including one located in Japan. (This isn't unusual, and ***Slate*** and the *Post* make no secret of it.)

Spooks can easily watch these tracking IDs as they flit across the Net, unprotected by any encryption, and then use the IDs to build the mother of all tracking databases. The NSA collects vast amounts of international Internet traffic, and it retains the metadata —including tracking IDs—**for at least a year.**

Unique identifiers solve many surveillance problems. What if several users share an Internet connection? Use tracking IDs to tell them apart. What if a user moves from home to a coffee shop or between cell towers? Follow the tracking IDs. What if you need to pinpoint a computer break-in? Aim at the target's tracking IDs. None of this requires the cooperation—or even awareness—of the tracking companies.

Geolocation is yet another freebie from the private sector. An Internet address provides only a rough estimate of a device's location; greater precision requires access to hardware features like GPS or Wifi. What spy agency would risk tapping directly into devices' GPS or Wifi chips? They don't need to—advertising and analytics software queries the onboard sensors, then phones home with an unencrypted and precise location. One NSA program, HAPPYFOOT, appears specifically designed to take advantage of this data.

The proliferation of third-party trackers also increases the reach of Internet surveillance. No government, not even the United States, can monitor every network path. Most Web pages include multiple third parties, each typically contacted through

a different route, giving spies more places to capture user activity. What's more, the largest third parties are in the United States, where the NSA's technical capabilities are at their zenith. Even if you're outside the United States and viewing a local webpage, for example, there might be a tipoff to an American advertiser. And the NSA.

If online services don't like this, they can go beyond lobbying for legal changes—useful as that is—and upgrade their technology. Tracking servers can switch to HTTPS, the secure, encrypted version of the Web's protocol. The **expert consensus** seems to be that even the NSA cannot accomplish mass surveillance of encrypted network traffic; HTTPS would put tracking IDs beyond a bulk eavesdropper's reach.

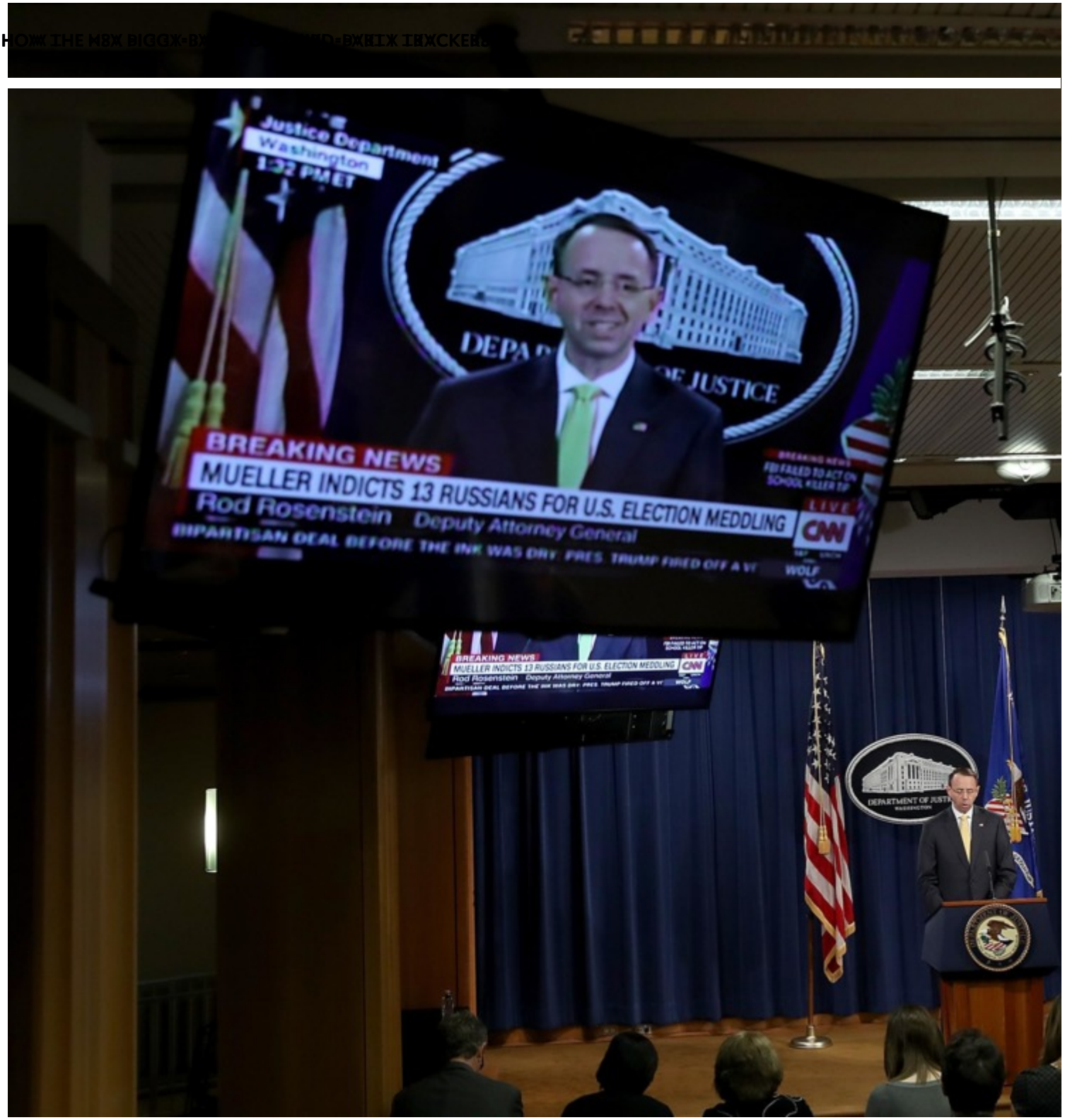
But technical security is not enough. The NSA can legally compel an American company to disclose records about *any* foreigner, with no individualized judicial review and scant transparency. The legal process is slower and more cumbersome than technical surveillance, to be sure, but still leaves much of the globe at risk. And the NSA has demonstrated it knows how to expedite the legal process using technology—that's precisely what the PRISM program does. As long as companies collect and retain tracking data, there will be a risk of disclosure through legal process, and users, especially those overseas, will be wary.

Future Tense *is a partnership of* ***Slate, New America****, and* ***Arizona State University****.*

What Good Is an Indictment for Online Election Meddling?

The U.S. keeps filing indictments for cyberconflicts, even though nothing ever comes from them.

By Josephine Wolff



U.S. Deputy Attorney General Rod Rosenstein announces the indictment of 13 Russian nationals and three Russian org

On Friday, Robert Mueller filed the first charges alleging election interference in his ongoing investigation of the 2016 presidential election. The **37-page indictment** alleges that 13 people and three companies in Russia committed illegal acts of aggravated identity theft, conspiring to commit wire fraud and bank fraud, and conspiring to defraud the United States. It's a fascinating read because of the details it reveals about the operations of Russia's election interference operation. But just like

the U.S. government's other attempts to respond to Russian interference in the election, the charges are a largely symbolic gesture likely to yield no real results or serious consequences for the accused.

Filing indictments seems to have become the United States' fallback response to international cyberconflicts despite the fact that, time and again, their attempts to **charge Chinese military officers** or **Russian government officials** for conducting cyberespionage have met with no success. It's understandable that the U.S. government is more comfortable resorting to established legal mechanisms than retaliating in kind when it comes to online manipulation and espionage, especially since those are exactly the activities it is trying to condemn and render less acceptable in the international ecosystem. And it's certainly possible that behind the scenes there are other, covert retaliatory measures that the public doesn't know about—but even if they are occurring, those activities won't serve as a deterrent to other would-be election meddlers so long as no one knows about them. So at least from a public-facing standpoint, at a certain point it starts to look like the United States is playing by a completely different, outdated set of rules that can never keep pace with Russia's willingness to explode conventions.

Russia has always been less cautious than most other countries when it comes to using the internet against its adversaries in new and creative ways. In 2007, Russia was believed to be behind massive **denial-of-service attacks directed at Estonia.** In 2008, the Russian government coordinated its military strike on Georgia with a series of **targeted cyberattacks on Georgian websites and infrastructure.** Ten years later, most other nations still haven't used their cyber capabilities that overtly or aggressively, but, as Mueller's indictment makes clear, that has not in any way deterred Russia from continuing to wield the internet with impunity.

CONTINUE READING