The Washington Post

The Switch

NSA uses Google cookies to pinpoint targets for hacking

By Ashkan Soltani, Andrea Peterson, and Barton Gellman December 10, 2013

The National Security Agency is secretly piggybacking on the tools that enable Internet advertisers to track consumers, using "cookies" and location data to pinpoint targets for government hacking and to bolster surveillance.

The agency's internal presentation slides, provided by former NSA contractor Edward Snowden, show that when companies follow consumers on the Internet to better serve them advertising, the technique opens the door for similar tracking by the government. The slides also suggest that the agency is using these tracking techniques to help identify targets for offensive hacking operations.

For years, privacy advocates have raised concerns about the use of commercial tracking tools to identify and target consumers with advertisements. The online ad industry has said its practices are innocuous and benefit consumers by serving them ads that are more likely to be of interest to them.

The revelation that the NSA is piggybacking on these commercial technologies could shift that debate, handing privacy advocates a new argument for reining in commercial surveillance.

According to the documents, the NSA and its British counterpart, GCHQ, are using the small tracking files or "cookies" that advertising networks place on computers to identify people browsing the Internet. The intelligence agencies have found particular use for a part of a Google-specific tracking mechanism known as the “PREF” cookie. These cookies typically don't contain personal information, such as someone's name or e-mail address, but they do contain numeric codes that enable Web sites to uniquely identify a person's browser.

In addition to tracking Web visits, this cookie allows NSA to single out an individual's communications among the sea of Internet data in order to send out software that can hack that person's computer. The slides say the cookies are used to "enable remote exploitation," although the specific attacks used by the NSA against targets are not addressed in these documents.

The NSA's use of cookies isn't a technique for sifting through vast amounts of information to find suspicious behavior; rather, it lets NSA home in on someone already under suspicion - akin to when soldiers shine laser pointers on a target to identify it for laser-guided bombs.

Separately, the NSA is also using commercially gathered information to help it locate mobile devices around the world, the documents show. Many smartphone apps running on iPhones and Android devices, and the Apple and Google operating systems themselves, track the location of each device, often without a clear warning to the phone's owner. This information is more specific than the broader location data the government is collecting from cellular phone networks, as reported by the Post last week.

"On a macro level, 'we need to track everyone everywhere for advertising' translates into 'the government being able to track everyone everywhere,'" says Chris Hoofnagle, a lecturer in residence at UC Berkeley Law. "It's hard to avoid."

These specific slides do not indicate how the NSA obtains Google PREF cookies or whether the company cooperates in these programs, but other documents reviewed by the Post indicate that cookie information is among the data NSA can obtain with a Foreign Intelligence Surveillance Act order. If the NSA gets the data that way, the companies know and are legally compelled to assist.

The NSA declined to comment on the specific tactics outlined in this story, but an NSA spokesman sent the Post a statement: "As we've said before, NSA, within its lawful mission to collect foreign intelligence to protect the United States, uses intelligence tools to understand the intent of foreign adversaries and prevent them from bringing harm to innocent Americans."

Google declined to comment for this article, but chief executive Larry Page joined the leaders of other technology companies earlier this week in calling for an end to bulk collection of user data and for new limits on court-approved surveillance requests. "The security of users' data is critical, which is why we've invested so much in encryption and fight for transparency around government requests for information," Page said in a statement on the coalition's Web site. "This is undermined by the apparent wholesale collection of data, in secret and without independent oversight, by many governments around the world."

How consumers are tracked online

Internet companies store small files called cookies on users' computers to uniquely identify them for ad-targeting and other purposes across many different Web sites. This advertising-driven business model pays for many of the services, like e-mail accounts, that consumers have come to expect to have for free. Yet few are aware of the full extent to which advertisers, services and Web sites track their activities across the Web and mobile devices. These data collection mechanisms are invisible to all but the most sophisticated users -- and the tools to opt-out or block them have limited effectiveness.

Privacy advocates have pushed to create a "Do Not Track" system allowing consumers to opt out of such tracking. But Jonathan Mayer of Stanford's Center for Internet and Society, who has been active in that push, says "Do Not Track efforts are stalled out." They ground to a halt when the Digital Advertising Alliance, a trade group representing online ad companies, abandoned the effort in September after clashes over the proposed policy. One of the primary issues of contention was whether consumers would be able to opt out of all tracking, or just not be served advertisements based on tracking.

Some browsers, such as Apple's Safari, automatically block a type of code known as "third-party cookies," which are often placed by companies that advertise on the site being visited. Other browsers such as Mozilla's Firefox are also experimenting with that idea. But such settings won't prevent users from receiving cookies directly from the primary sites they visit or services they use.

Google's PREF Cookie

Google assigns a unique PREF cookie anytime someone's browser makes a connection to any of the company's Web properties or services. This can occur when consumers directly use Google services such as Search or Maps, or when they visit Web sites that contain embedded "widgets" for the company's social media platform Google Plus. That cookie contains a code that allows Google to uniquely track users to "personalize ads" and measure how they use other Google products.

Given the widespread use of Google services and widgets, most Web users are likely to have a Google PREF cookie even if they've never visited a Google property directly.

That PREF cookie is specifically mentioned in an internal NSA slide, which reference the NSA using GooglePREFID, their shorthand for the unique numeric identifier contained within Google's PREF cookie. Special Source Operations (SSO) is an NSA division that works with private companies to scoop up data as it flows over the Internet's backbone and from technology companies' own systems. The slide indicates that SSO was sharing information containing "logins, cookies, and GooglePREFID" with another NSA division called Tailored Access Operations, which engages in offensive hacking operations. SSO also shares the information with the British intelligence agency GCHQ.

"This shows a link between the sort of tracking that's done by Web sites for analytics and advertising and NSA exploitation activities," says Ed Felten, a computer scientist at Princeton University. "By allowing themselves to be tracked for analytic or advertising at least some users are making themselves more vulnerable to exploitation."

This isn't the first time Google cookies have been highlighted in the NSA's attempts to identify targets to hack. A presentation released in October by the Guardian called "Tor Stinks" indicates that the agency was using cookies for DoubleClick.net, Google's third-party advertising service, in an attempt to identify users of the Internet anonymization tool Tor when they switched to regular browsing. "It's similar in the sense that you see the use of an unique ID in the cookie to allow an eavesdropper to connect the activities of a user over time," says Felten.

Leaked location data

Another slide indicates that the NSA is collecting location data transmitted by mobile apps to support ad-targeting efforts in bulk. The NSA program, code-named HAPPYFOOT, helps the NSA to map Internet addresses to physical locations more precisely than is possible with traditional Internet geolocation services.

Many mobile apps and operating systems use location-based services to help users find restaurants or establishments nearby. In fact, even when GPS is disabled, most smart phones silently determine their location in the background using signals from Wi-Fi networks or cellular towers.

And apps that do not need geo-location data may still collect it anyway to share with third-party advertisers. Just last week, the Federal Trade Commission announced a settlement for a seemingly innocuous flashlight app that allegedly leaked user location information to advertisers without consumers' knowledge.

Apps transmit their locations to Google and other Internet companies because ads tied to a precise physical location can be more lucrative than generic ads. But in the process, they appear to tip off the NSA to a mobile device's precise physical location. That makes it easier for the spy agency to engage in the sophisticated tracking techniques the Post described in a story Dec. 4.

Implications for privacy

The disclosures about NSA practices reveal the dilemma facing online companies, which have faced a backlash against tracking for commercial purposes and their role in government surveillance.

"If data is used and it stops the next 9/11 our fellow citizens wouldn't have any problem with it no matter what it is," says Stuart P. Ingis, General Counsel at the Digital Advertising Association. But he says that it is a balancing act to pursue those bad actors "while at the same time preserving the civil liberties."

Other defenders of online advertising companies have argued it is unfair to conflate private companies' ad-tracking activities with the NSA activities revealed in the Snowden leaks. Marvin Ammori, a lawyer who advises technology companies including Google on surveillance issues, wrote in USA Today that "limiting bulk data collection by private companies - whether they advertise or not - would do little or nothing to limit the NSA."

Felten disagrees, noting that the latest documents show that "the unique identifiers that are being placed on users' computers are not only being used by analytic and advertising companies, but also being used by the NSA for targeting." He also says that there are things those companies could do to protect their users from the type of attacks described in the slides, like "not sending tracking IDs, or at least not sending them in the clear" without a layer of encryption.

Similarly, he says, "browser makers can help by giving users better control over the use of third-party tracking cookies and by making sure that their browsers are not sending unique IDs as a side effect of their safe-browsing behavior."

Stanford's Mayer says the revelations suggest the need for limits on the data that companies collect about consumers. "There's increasingly a sense that giving consumers control over the information they share with companies is all the more important," he says, "because you're also giving them control over the information they share with government."

Soltani is an independent security researcher and consultant.

Read the annotated documents here.

Soltani explains how the NSA uses Google cookies in a PostTV interview.