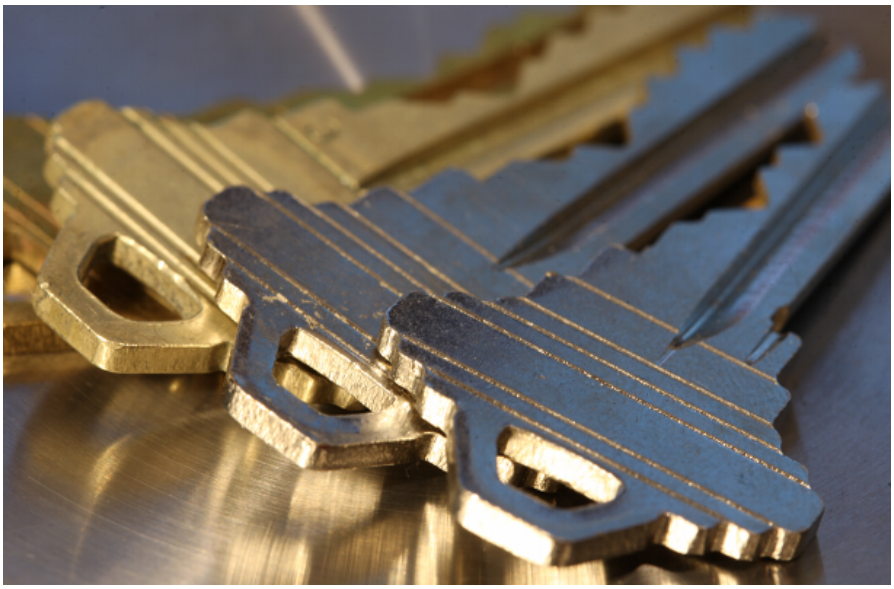
CNET News

Feds put heat on Web firms for master encryption keys

Whether the FBI and NSA have the legal authority to obtain the master keys that companies use for Web encryption remains an open question, but it hasn't stopped the U.S. government from trying.

by **Declan McCullagh** | July 24, 2013 4:00 AM PDT



Large Internet companies have resisted the government's demands for encryption keys requests on the grounds that they go beyond what the law permits, according to one person who has dealt with these attempts.

(Credit: Declan McCullagh)

The U.S. government has attempted to obtain the master encryption keys that Internet companies use to shield millions of users' private Web communications from eavesdropping.

These demands for master **encryption keys [http://www.cnet.com/8301-13578_3-57591560-38/facebooks-outmoded-web-crypto-opens-door-to-nsa-spying/]**, which have not been disclosed previously, represent a technological escalation in the clandestine methods that the FBI and the National Security Agency employ when conducting electronic surveillance against Internet users.

If the government obtains a company's master encryption key, agents could decrypt the contents of communications intercepted through a wiretap or by invoking the potent surveillance authorities of the **Foreign Intelligence Surveillance Act [http://www.cnet.com/8301-13578_3-57588337-38/no-evidence-of-nsas-direct-access-to-tech-companies/]**. Web encryption -- which often appears in a browser with a HTTPS lock icon when enabled -- uses a technique called SSL, or Secure Sockets Layer.

"The government is definitely demanding SSL keys from providers," said one person who has responded to government attempts to obtain encryption keys. The source spoke with CNET on condition of anonymity.

The person said that large Internet companies have resisted the requests on the grounds that they go **beyond what the law permits [http://www.cnet.com/8301-13578_3-57593538-38/how-the-u.s-forces-net-firms-to-cooperate-on-surveillance/]**, but voiced concern that smaller companies without well-staffed legal departments might be less willing to put up a fight. "I believe the government is

beating up on the little guys," the person said. "The government's view is that anything we can think of, we can compel you to do."

A Microsoft spokesperson would not say whether the company has received such requests from the government. But when asked whether Microsoft would turn over a master key used for Web encryption or **server-to-server e-mail encryption [http://www.cnet.com/8301-13578_3-57590389-38/how-web-mail-providers-leave-door-open-for-nsa-surveillance/]** , the spokesperson replied: "No, we don't, and we can't see a circumstance in which we would provide it."

Google also declined to disclose whether it had received requests for encryption keys. But a spokesperson said the company has "never handed over keys" to the government, and that it carefully reviews each and every request. "We're sticklers for details -- frequently pushing back when the requests appear to be fishing expeditions or don't follow the correct process," the spokesperson said.

Sarah Feinberg, a spokeswoman for Facebook, said that her employer has not received requests for encryption keys from the U.S. government or other governments. In response to a question about divulging encryption keys, Feinberg said: "We have not, and we would fight aggressively against any request for such information."

Apple, Yahoo, AOL, Verizon, AT&T, Time Warner Cable, and Comcast declined to respond to queries about whether they would divulge encryption keys to government agencies.

Richard Lovejoy, a director of the Opera Software subsidiary that operates **FastMail [https://www.fastmail.fm/]** , said: "Our interpretation is that we are prohibited by law from releasing our SSL key. In the event that we received such a request, we would refuse, for both legal and ethical reasons." Releasing the SSL key would be nearly "equivalent to allowing interception on all our users, which is clearly illegal," Lovejoy said.

Encryption used to armor Web communications was largely adopted not because of fears of NSA surveillance -- but because of the popularity of open, insecure Wi-Fi networks. The "Wall of Sheep," which highlights passwords transmitted over networks through unencrypted links, has become a **fixture [http://www.cnet.com/8301-1009_3-10010450-83.html]** of computer security conventions, and Internet companies began **adopting SSL in earnest [http://www.cnet.com/8301-1023_3-9999473-93.html]** about three years ago.

"The requests are coming because the Internet is very rapidly changing to an encrypted model," a former Justice Department official said. "SSL has really impacted the capability of U.S. law enforcement. They're now going to the ultimate application layer provider."

An FBI spokesman declined to comment, saying the bureau does not "discuss specific strategies, techniques and tools that we may use."

NSA director Keith Alexander, shown here at a Washington, D.C. event this month, has said that encrypted data are "virtually unreadable."

(Credit: Getty Images)

Top secret NSA documents leaked by former government contractor Edward Snowden suggest an additional reason to ask for master encryption keys: they can aid bulk surveillance conducted **through the spy agency's fiber taps [http://www.cnet.com/8301-13578_3-57591391-38/surveillance-partnership-between-nsa-and-telcos-points-to-at-t-verizon/]** .

One of the **leaked PRISM slides [http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html]** recommends that NSA analysts collect communications "upstream" of data centers operated by Apple, Microsoft, Google, Yahoo, and other Internet companies. That procedure relies on a FISA order requiring backbone providers to aid in "collection of communications on fiber cables and infrastructure as data flows past."

Mark Klein, who worked as an AT&T technician for over 22 years, **disclosed [http://www.cnet.com/8301-10784_3-6058346-7.html]** in 2006 (**PDF [https://www.eff.org/files/filenode/att/SER_klein_decl.pdf]**) that he met with NSA officials and witnessed domestic Internet traffic being "diverted" through a "splitter cabinet" to secure room 641A in one of the company's San Francisco facilities. Only NSA-cleared technicians were allowed to work on equipment in the SG3 secure room, Klein said, adding that he was told similar fiber taps existed in other major cities.

Related posts

- **School district hires company to follow kids' Facebook, Twitter [http://www.cnet.com/8301-852_3-57600251-71/school-district-hires-company-to-follow-kids-facebook-twitter/]**
- **Assange's brilliant mullet-wearing, classic-miming video [http://www.cnet.com/8301-17852_3-600164-71/assanges-brilliant-mullet-wearing-classic-miming-video/]**
- **Matt Damon: Edward Snowden did a great thing [http://www.cnet.com/8301-17852_3-600048-71/matt-damon-edward-snowden-did-a-great-thing/]**
- **NSA paid tech firms over Prism, says latest Snowden leak [http://www.cnet.com/8301-578_3-57599952-38/nsa-paid-tech-firms-over-prism-says-latest-snowden-leak/]**
- **NSA admits to some deliberate privacy violations [http://www.cnet.com/8301-13578_3-599916-38/nsa-admits-to-some-deliberate-privacy-violations/]**

But an increasing amount of Internet traffic flowing through those fiber cables is now armored against surveillance using SSL encryption. Google **enabled [http://gmailblog.blogspot.com/2010/01/default-https-access-for-gmail.html]** HTTPS by default for Gmail in 2010, **followed soon after by [http://www.cnet.com/8301-27080_3-20022241-245.html]** Microsoft's Hotmail. Facebook **enabled encryption by default [https://developers.facebook.com/blog/post/2012/11/14/platform-updates--operation-developer-love/]** in 2012. Yahoo **now offers it [http://howto.cnet.com/8301-11310_39-57562895-285/how-to-secure-yahoo-mail-web-sessions-with-ssl/]** as an option.

"Strongly encrypted data are virtually unreadable," NSA director Keith Alexander told (**PDF [http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-091.pdf]**) the Senate earlier this year.

Unless, of course, the NSA can obtain an Internet company's private SSL key. With a copy of that key, a government agency that intercepts the contents of encrypted communications has the technical ability to decrypt and peruse everything it acquires in transit, although actual policies may be more restrictive.

One exception to that rule relies on a clever bit of mathematics called perfect forward secrecy. PFS uses temporary individual keys, a different one for each encrypted Web session, instead of relying on a single master key. That means even a government agency with the master SSL key and the ability to passively eavesdrop on the network can't decode private communications.

Google is the **only major Internet company to offer PFS [http://www.cnet.com/8301-13578_3-57591179-38/data-meet-spies-the-unfinished-state-of-web-crypto/]** , though Facebook is preparing to enable it by default.

Even PFS isn't complete proof against surveillance. It's possible to mount a more advanced attack, sometimes called a man-in-the-middle or active attack, and decode the contents of the communications.

A **Wired article [http://www.wired.com/threatlevel/2010/03/packet-forensics/]** in 2010 disclosed

that a company called Packet Forensics was marketing to government agencies a box that would do precisely that. (There is no evidence that the NSA performs active attacks as part of routine surveillance, and even those could be detected in some circumstances.)

The Packet Forensics brochure said that government agencies would "have the ability to import a copy of any legitimate key they obtain (potentially by court order)." It predicted that agents or analysts will collect their "best evidence while users are lulled into a false sense of security afforded by Web, e-mail or VOIP encryption."

With a **few exceptions [http://www.cnet.com/8301-13578_3-57594171-38/google-tests-encryption-to-protect-users-drive-files-against-government-demands/]** , even if communications in transit are encrypted, Internet companies typically do not encrypt e-mail or files stored in their data centers. Those remain accessible to law enforcement or the NSA through legal processes.

Leaked **NSA surveillance procedures [http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document]** , authorized by Attorney General Eric Holder, suggest that intercepted domestic communications are typically destroyed -- unless they're encrypted. If that's the case, the procedures say, "retention of all communications that are enciphered" is permissible.

Valerie Caproni, who was the FBI's general counsel at the time this file photo was taken, told Congress that the government needs "individualized solutions" when "individuals who put encryption on their traffic."

(Credit: Getty Images)

It's not entirely clear whether federal surveillance law gives the U.S. government the authority to demand master encryption keys from Internet companies.

"That's an unanswered question," said **Jennifer Granick [http://cyberlaw.stanford.edu/about/people/jennifer-granick]** , director of civil liberties at Stanford University's Center for Internet and Society. "We don't know whether you can be compelled to do that or not."

The government has attempted to use subpoenas to request copies of encryption keys in some cases, according to one person familiar with the requests. Justice Department **guidelines [http://www.justice.gov/atr/public/guidelines/206696.htm#IIIA1]** say subpoenas may be used to obtain information "relevant" to an investigation, unless the request is "unreasonably burdensome."

"I don't know anyone who would turn it over for a subpoena," said an attorney who represents Internet companies but has not fielded requests for encryption keys. Even a wiretap order in a criminal case would be insufficient, but a FISA order might be a different story, the attorney said. "I'm sure there's some logic in collecting the haystack."

Kurt Opsahl [https://www.eff.org/about/staff/kurt-opsahl] , a senior staff attorney at the **Electronic Frontier Foundation [https://www.eff.org/]** , challenged the notion that current law hands the government the power to demand master encryption keys. Even with a FISA order for the private

key, Opsahl said, the amount of technical assistance that a company must provide to the NSA or other federal agencies "has a limit."

Federal and state law enforcement officials have previously said encrypted communications were beginning to pose an obstacle to lawful surveillance. Valerie Caproni, the FBI's general counsel at the time, told a congressional hearing in 2011, according to a **transcript [http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg64581/html/CHRG-112hhrg64581.htm]** :

> Encryption is a problem, and it is a problem that we see for certain providers... For individuals who put encryption on their traffic, we understand that there would need to be some individualized solutions if we get a wiretap order for such persons... We are suggesting that if the provider has the communications in the clear and we have a wiretap order, that the provider should give us those communications in the clear.

"One of the biggest problems with compelling the [private key] is it gives you access to not just the target's communications, but all communications flowing through the system, which is exceedingly dangerous," said Stanford's Granick.

Last update, July 25 at 1 p.m. PT: *Added a response from FastMail, which arrived after this article was published. This article was previously updated to add additional comments from a Facebook representative saying the company has not received such requests.*

Disclosure: McCullagh is married to a Google employee not involved with this issue.

[http://www.cnet.com/profile/declan00/]

Cullagh [http://www.cnet.com/profile/declan00/]

ttp://www.mccullagh.org/] is the chief political correspondent for CNET. a reporter for Time and the Washington bureau chief for Wired and wrote the and Other People's Money column for CBS News' Web site.

- **[http://plus.google.com/112961607570158342254/]**