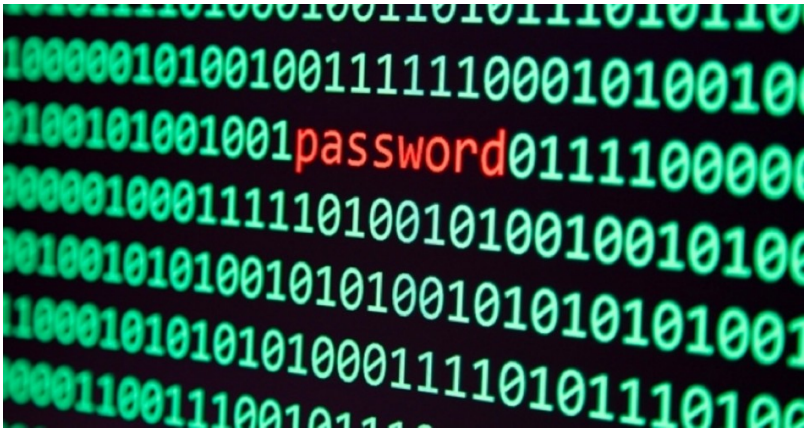
Written by **Warren Mass** on July 26, 2013

Federal Government Demands Internet Passwords



A story broken by CNET on July 25 stated that the U.S. government has "demanded" that major Internet companies provide federal agencies with their customers' passwords. The report identified the information as coming from two unidentified technology industry sources "familiar with these orders."

The report quoted two sources working in the high-tech industry, neither of whom wished to be identified. "I've certainly seen them ask for passwords,' said one Internet industry source who spoke on condition of anonymity. "We push back."

A second person, identified as someone who worked at a large Silicon Valley company, confirmed that it received legal requests from the federal government for stored passwords. Companies "really heavily scrutinize" these requests, the person said. "There's a lot of 'over my dead body.'"

The report revealed, again citing "a person familiar with the requests," that some of the federal government "orders" (not requests) have demanded more than a user's password but also the encryption algorithm and the so-called "salt." (An article in Wikipedia defines this term: "In cryptography, a salt is random data that are used as an additional input to a one-way function that hashes a password or passphrase…. The original intent of salting was primarily to defeat pre-computed rainbow table attacks that could otherwise be used to greatly improve the efficiency of cracking the hashed password database.") In other words, the federal government wants not only the key to the lock, but also the means to disarm the security protecting the lock, as well. Other government orders have demanded the secret question codes (e.g., "Who was your favorite teacher?") often associated with user accounts.

The report also cited an exchange with a spokesperson from Microsoft Corporation, who declined to divulge whether the company had received password requests or demands from the federal government. However, when the CNET writer asked whether Microsoft would divulge passwords, salts, or algorithms, the spokesperson replied: "No, we don't, and we can't see a circumstance in which we would provide it."

A spokesperson for Google also told CNET that the company had "never" provided the government with such information, stating: "We take the privacy and security of our users very seriously."

The report also quoted a statement from a Yahoo spokeswoman who said: "If we receive a request from law enforcement for a user's password, we deny such requests on the grounds that they would allow overly broad access to our users' private information. If we are required to provide information, we do so only in the strictest interpretation of what is required by law."

A reporter for *Business Insider* observed that this latest federal action "represents an even worse scenario than the one posited by National Security Agency (NSA) leaker Edward Snowden, who claimed

the feds have a program named PRISM that gives them access to the servers of Google, Facebook, Microsoft, and other major web providers. The companies have denied that such a program exists, saying they only respond to specific legal requests about individuals."

With government agencies such as the NSA easily able to obtain the best and most expensive computers needed to engage in password cracking, is it really necessary for them to demand the actual passwords and related data from Internet companies? Anyone who watches *Criminal Minds* has seen one of the show's characters, analyst Penelope Garcia, hack into databases with the ease of a kindergartener making a finger painting.

In an article posted on Hothardware.com on July 26, a writer named Joel Hruska offers the following observation:

> The CNET article [implies] that because websites liked LinkedIn and Twitter use a difficult hashing algorithm called bcrypt, it would be extremely expensive for the NSA to brute-force these passwords. The current estimate for the cost of brute-forcing a 10-character password in a single day is about $60 million dollars — not the $1.2 billion originally estimated in 2009.
>
> Not only is it well within the NSA's capability to build a $60 million dollar computer dedicated to password cracking, empirical evidence shows it's not necessary. When LinkedIn password hashes leaked earlier this year, upwards of 100 million of them had been cracked in days. Not by brute-force — that's the stupid, difficult, work of last resort. Instead, hackers used sophisticated hybrid attack methods that blend dictionary approaches and password-cracking rules with "try everything and see what works" algorithms. Combine that with off-the-shelf GPU hardware, and the reality is that very few passwords would take anything like that much cash to crack.

Hruska concludes his article: "With multiple requests to the government for more disclosures still pending, it's encouraging to see information like this leaking out — it's the only way to chip apart the culture of secrecy that's ossified in the 12 years since 9/11."

As was reported in *The New American* on July 24, Rep. Justin Amash (R-Mich.) added an amendment to the defense appropriations bill (co-sponsored by Rep. John Conyers [D-Mich.]) that would have revoked authority "for the blanket collection of records under the Patriot Act. It would also have barred the NSA and other agencies from using Section 215 of the Patriot Act to collect records, including telephone call records, that pertain to persons who are not subject to an investigation under Section 215" of the Patriot Act.

So alarmed was the White House that Amash's amendment might pass, that it issued a statement on July 23 opposing it that read, in part:

> In light of the recent unauthorized disclosures [by Edward Snowden], the President has said that he welcomes a debate about how best to simultaneously safeguard both our national security and the privacy of our citizens.
>
> However, we oppose the current effort in the House to hastily dismantle one of our Intelligence Community's counterterrorism tools. This blunt approach is not the product of an informed, open, or deliberative process. We urge the House to reject the Amash Amendment, and instead move forward with an approach that appropriately takes into account the need for a reasoned review of what tools can best secure the nation.

Amash tweeted his reaction late on July 23: "When's the last time a president put out an emergency

statement against an amendment? The Washington elites fear liberty. They fear you."

The next day, the House narrowly defeated the Amash amendment, 207-217. (For a roll call on the vote, click here.)

The unusual make-up of the vote, considering the White House's strong lobbying against the amendment, was noted in an article posted by *The New American* on July 25, in which writer Joe Wolverton noted:

> An analysis of the roll call reveals that a majority of Democrats voted in favor of restricting the Obama administration's wholesale surveillance of Americans, while a majority of the GOP voted to uphold the NSA's unconstitutional surveillance of all electronic communications.

Rep. Conyers, who scored an anemic 30 percent on *The New American's* recent "Freedom Index" (PDF), seemed to hit the nail on the head regarding the Amash amendment, perhaps proving the old adage that "even a stopped clock tells the right time twice a day." He said:

> It is unfortunate that so much of Congress and the media's focus is on the whereabouts of Edward Snowden. We should focus our time and attention on ensuring that law-abiding Americans are not unnecessarily subject to intrusive surveillance; making sure our media organizations are not targeted merely for informing the public; closing Guantanamo and releasing those individuals who pose us no harm; and demanding that legal safeguards are in place with respect to our government's shortsighted use of drones. These are the overriding, critical issues facing the Congress, not the whereabouts or motives of Edward Snowden.

Related articles:

Vote on Amash Amendment Reveals Ruse of Two-Party System

Rep. Amash: "Washington Elites Fear Liberty"