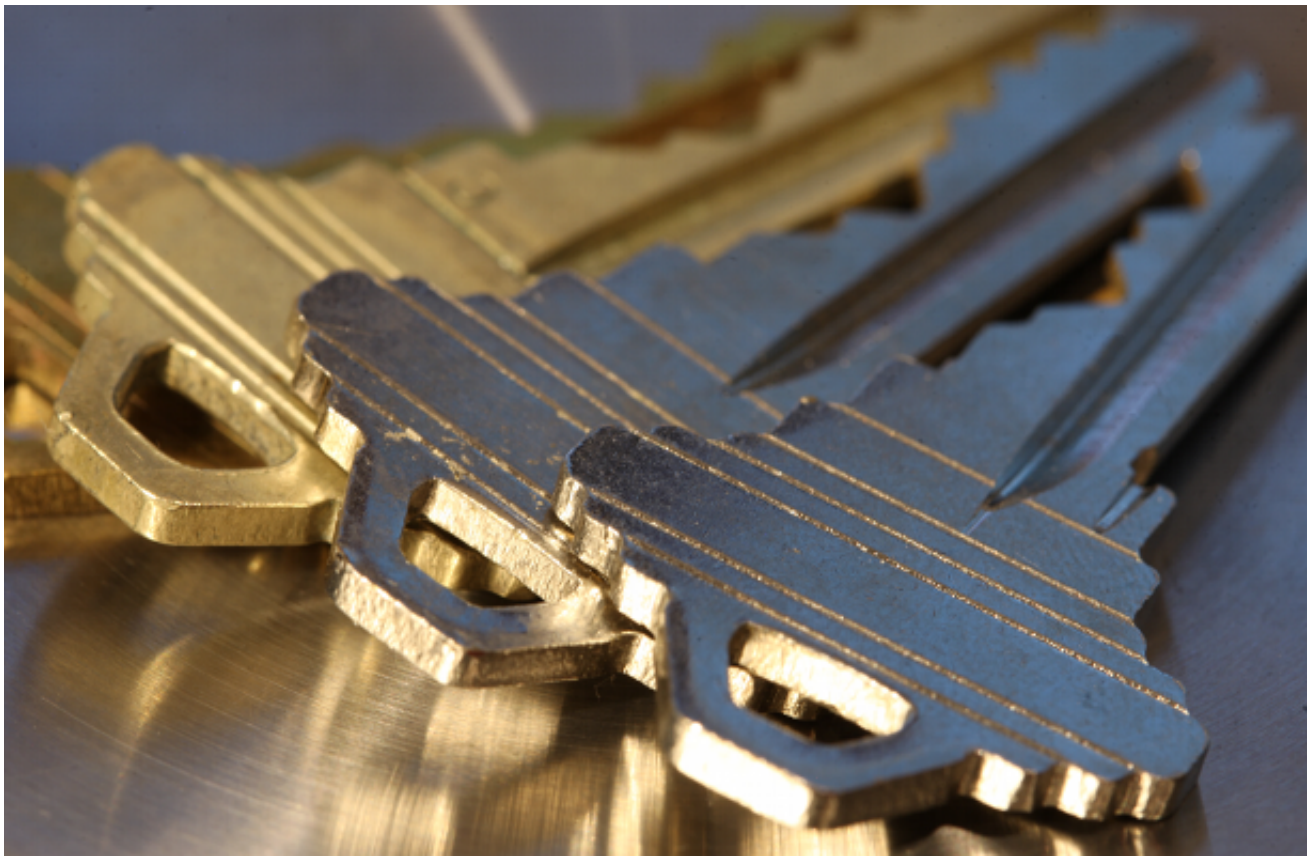
Feds put heat on Web firms for master encryption keys

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

- **Follow @declanm**



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

- **FBI pressures Internet providers to install surveillance software [http://www.cnet.com/8301-13578_3-57596791-38/fbi-pressures-internet-providers-to-install-surveillance-software/]**
- **FBI said to be taking a hacker approach to spying [http://www.cnet.com/8301-1009_3-57596672-83/fbi-said-to-be-taking-a-hacker-approach-to-spying/]**
- **Internet Webcam service Dropcam nets $30M in funding [http://www.cnet.com/8301-1023_3-57596228-93/internet-webcam-service-dropcam-nets-$30m-in-funding/]**
- **Feds tell Web firms to turn over user account passwords [http://www.cnet.com/8301-13578_3-57595529-38/feds-tell-web-firms-to-turn-over-user-account-passwords/]**
- **House narrowly rejects bid to curb NSA domestic surveillance [http://www.cnet.com/8301-13578_3-57595391-38/house-narrowly-rejects-bid-to-curb-nsa-domestic-surveillance/]**

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.html]** :

> **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/]

About Declan McCullagh [http://www.cnet.com/profile/declan00/]

Declan McCullagh [http://www.mccullagh.org/] is the chief political correspondent for CNET. Declan previously was a reporter for Time and

bureau chief for Wired and wrote the Taking Liberties
r People's Money column for CBS News' Web site.

- **google.com/112961607570158342254/]**
- **Follow @declanm [http://www.twitter.com/declanm]**
-

You May Also Like

Woman buys two iPhones for $1,300, gets only apples (really)

CNET

[http://news.cnet.com/8301-13579_3-57596900-37/woman-buys-two-iphones-for-$1300-

gets-only-apples-really/]

Foxconn brushes off claims of pollution in China

CNET

[http://news.cnet.com/8301-1001_3-57596979-92/foxconn-brushes-off-claims-of-

pollution-in-china/]

Donald Trump Tells Americans to Prepare for "Financial Ruins"

Money News

[http://www.moneynews.com/Archives/Trump-Aftershock-American-

[http://www.moneynews.com/Archives/Trump-Aftershock-American-

Economy/2012/11/06/id/462985?PROMO_CODE=103FC-1] Amazing Auctions Let You Buy iPads and Other Electronics for Under $40

First To Know

[http://firsttoknow.com/article/?ag=1297&utm_source=n_t&utm_campaign=how-to-find-ipads-for-%2-17085]

about these links

[]

Member Comments

116 Comments/

59 people following

Log in []

Commenting FAQs [http://www.cnet.com/2706-1_1-1954.html] / Guidelines [http://www.cnet.com/2706-1_1-1947.html]

Post to:

+ Follow conversation Post Comment As...

Newest [] /Oldest [] /Top Comments []

NoTrustDotOrg [http://www.cnet.com/profile/NoTrustDotOrg] Aug 3, 2013

This makes clear the need for an organization like notrust_dot_org. It's time for he Web's users to demand from Web companies that all private communications be encrypted at the browser using strong public key schemes toward eliminating wholesale abuses of user privacy. The only data Web companies should be exposed

to in the clear should be data REQUIRED for serving users or information that users post for public consumption (e.g., public comments such as this one). In the end, the loss of privacy on a wholesale level will expose society to abuses by leaders (current or future) of a tyrannical bent, and will result in a squelching of the free speech and association so essential to the liberty of any truly free people. Just imagine what access to all private communication would have meant to a Mussolini, a Stalin, an (*insert your most despised despot here*). ... not a pretty scene.

/ like []reply []

nniebur [http://www.cnet.com/profile/nniebur] Jul 31, 2013

Seems to me that if one were to communicate the old fashioned way through writing a letter and sending it via snail mail, it would take a court order for the gov to intercept and read through. Even then one would have a notion that their mail had been tampered with when they received it by the condition of the envelope. The gov never had a program of intercepting all written and post mailed communication so why should they be able to do so just because the medium is electronic?

/ like []reply []

gbpgd [http://www.cnet.com/profile/gbpgd] Jul 26, 2013

Can you imagine someone putting Anthony Weiner's phone sex or sexting messages on the internet ? Even sexy emails ?

that is the power the Feds and the NSA will wield over every politician .

/ like []reply []

CertiVox [http://www.cnet.com/profile/CertiVox] Jul 26, 2013

Start with the basics. Usr/pswd is 40 year old technology underpinning the security of the internet - madness. This why usernames / passwords MUST be obviated for

other forms of electronic identification.

M-Pin is one such protocol, and you can see it in action at the CertiVox website. It's HTML5 based, and uses an ATM style user experience and cryptography so there is no username and password at the front end. More importantly, the M-Pin server has no usr/pswd database, just one cryptographic leakproof key. It's impossible to turn over any usr/pswd because it doesn't exist! It's been architected from the ground up with a cryptographer's mind set: TRUST NO ONE.

It's possible to innovate our way out of this mess but people need to wake up to the fact they we are one step away from a police state. It's all well and good if we have a benign government, but can you imagine someone like Richard Nixon back in charge with the NSA's current capability? Scary.

Full disclosure: I'm the CEO of CertiVox, the team that makes M-Pin.

/ **like []reply []**

Scrummyinthetummy [http://www.cnet.com/profile/Scrummyinthetummy] Jul 26, 2013

I think this goes beyond just keeping there eyes on the bad guys. Maybe a obsession with control I would think? This is what we know…what don't we know?

/ **like []reply []**

Cowicide [http://www.cnet.com/profile/Cowicide] Jul 25, 2013

Lindsey Graham should put the logos of Northrop Grumman, Lockheed Martin and Boeing, etc. on his forehead to make it clearer whose side he's really on. It's not the American public, it's war profiteers who despise the American public and are very willing to sacrifice our lives, liberties and treasure for their own greedy profits.

The war profiteers are who Lindsey Graham really represents:
http://www.huffingtonpost.com/robert-greenwald/mee... [http://www.huffingtonpost.com/robert-greenwald/meet-the-001-percent-war_b_1034971.html]

Lindsey Graham is a traitor to the American people. This isn't about our security, it's about protecting corrupt profits.

http://www.washingtonsblog.com/2013/06/the-dirty-l... [http://www.washingtonsblog.com/2013/06/the-dirty-little-secret-about-nsa-spying-it-doesnt-work.html]

Daily Caller: So what are they doing with all of this information? If they can't stop the Boston marathon bombing, what are they doing with it?

Binney: Well again, they're putting an extra burden on all of their analysts. It's not something that's going to help them; it's something that's burdensome. There are ways to do the analysis properly, but they don't really want the solution because if they got it, they wouldn't be able to keep demanding the money to solve it. I call it their business statement, "Keep the problems going so the money keeps flowing." It's all about contracts and money.

/ **like []reply []**

Chris737j2 [http://www.cnet.com/profile/Chris737j2] Jul 25, 2013

The majority of one social site controlled by the Government, by the Government. The news is the least honest outlet, for reporting, seeing facebook inc. still clause they backed out it's first partner, and refused to do-but a spin off several stories- of facts. No one wants spies or actual personal stories about actual people-just the benefits,profits and attention.That's the fault of? Some elected leaders want full access of your worth,intention,vote,

/ **like []reply []**

SasparillaFizz [http://www.cnet.com/profile/SasparillaFizz] Jul 25, 2013

I love this:

>> "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. <<

Yeah, the Emperor of the NSA, who has directly lied under oath numerous times...we should trust what he says...right...

Does anyone have any doubt (based on what we've found out so far) that if these companies don't turn over their SSL master keys to the U.S. intelligence Empire when asked (and it seems most of the big ones won't do that) - that the NSA or one of their friends would just obtain them illegally either via direct attacks and or people on the inside of these companies.

/ **like []reply []**

jdnoonan1972 [http://www.cnet.com/profile/jdnoonan1972] Jul 25, 2013

The US government is going to kill the US tech industry. "Land of the free" my ass. We have become very close to what I was taught the Soviet Union was when I was a kid.

/ 1**like []reply []**

eccles1214 [http://www.cnet.com/profile/eccles1214] Jul 25, 2013

Use email and web providers that are based in the EU, especially on the continent side (not UK or Ireland), as countries such as Germany and Switzerland have more stringent privacy protections.

/ 1**like []reply []**

mikehenken [http://www.cnet.com/profile/mikehenken] Jul 25, 2013

@eccles1214 [http://www.cnet.com/profile/eccles1214] Right. Because there

have been no countries in Europe accused of spying on their citizens.. smh..

This is not an "U.S." problem, this is a problem across the world with dozens of countries.

/ like []reply []

simonf123 [http://www.cnet.com/profile/simonf123] Jul 25, 2013

Its a shame that the focus is always on Government and not the vast numbers of people who send email in clear. If there is genuine concern about privacy from Government then considerable numbers in the legal sector would bother to encrypt their email. There are lots of good products around such as PKI, PGP, Mkryptor, Egress etc. They will all help. Yes it is wrong that the government is invading privacy in this way but given only very small amounts of email traffic is encrypted I would be more concerned with bringing the US up to standard.

/ like []reply []

xcopy [http://www.cnet.com/profile/xcopy] Jul 25, 2013

@simonf123

I think you can't see the forest for the trees. The concern is why SHOULD people have to encrypt their email to keep the US "secret police" (Gestapo, Stasi, KGB, et. al.) out of their business?

As to your other point, do you really think those encryption routines will keep the govt out of your mail? If so, you'd be wrong. The real problem is the bunch of lying and corrupt individuals that are "protecting" us, and complicit corporations of course.

Again, Ben Franklin's security comment comes to mind. You should find it, read it, and take it to heart. We are never going to be free again unless/until we stop our own government.

/ 2like []reply []

simonf123 [http://www.cnet.com/profile/simonf123] Jul 25, 2013

@xcopy [http://www.cnet.com/profile/xcopy] I agree. This is more down to my poor communication. The principle of privacy in debate here is clear. One should not have to protect oneself from Government. You have my support there and there are clear constitutional issues at play here. In the UK we have exactly the same issue too. There is a bill being proposed to snoop on email communications (not content they promise). There is a big debate here.

My point I was trying to make (clearly badly) is that Government is not the only people after our data. Cyber crime in the UK is rising fast and we are facing the reality that a lot of data is finding itself in the hands of organised crime, most often based abroad. Crimes are therefore committed by criminals well outside of the effective reach of the justice system here. I suspect the same is true of the US.

In the UK, the media is very focused on the Government snooping and the right to privacy. But very little is done to educate the masses on criminal snooping.

This is not an either or matter. Society as a whole needs to be protected against the risks of over reaching Government officials AND the risks of data loss to criminals.

Effective or otherwise, at least the Government has to respond to such questions and there are routes to hold them accountable for their encroachment in our private lives. We have no such route to debate this with organised crime. We need to raise the awareness of the latter as much as the former.

I hope that clarifies my position.

/ like []reply []

xcopy [http://www.cnet.com/profile/xcopy] Jul 25, 2013

@simonf123@xcopy

Yes, thank you, it clarifies your position very well, and I agree with you.

You're right, we all face potential threats from "bad actors" (organized crime, hackers, etc.) and encryption may help slow them down a little. With some

diligence, we can often avoid most of these actors - though we can't protect ourselves when they hack a site where we store data.

As to the UK privacy debate you're facing, Franklin's words from 1775 (as I alluded to previously) might apply equally well there.

"They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety".

http://en.wikiquote.org/wiki/Benjamin_Franklin [http://en.wikiquote.org/wiki/Benjamin_Franklin]

It's a pity we have no more statesmen in this country, and our citizens are too busy to fight off what is happening under the guise of "safety".

/ like []reply []

man_in_la2000 [http://www.cnet.com/profile/man_in_la2000] Jul 25, 2013

Master Encryption keys are a GIANT security risk , the android one is already out in wild

/ 2like []reply []

Lerianis6 [http://www.cnet.com/profile/Lerianis6] Jul 25, 2013

@man_in_la2000 [http://www.cnet.com/profile/man_in_la2000]

Exactly. There should NEVER be a master security key that can override or decrypt everything encrypted by a standard in question.

That is the whole reason that Freenet DOESN'T have a master security key. Same thing for Truecrypt and BestCrypt.

/ like []reply []

anywherehome2 [http://www.cnet.com/profile/anywherehome2] Jul 25, 2013

@man_in_la2000 while iPhone you can sometimes hack by just visiting some www site :)

/ like []reply []

carolamrt [http://www.cnet.com/profile/carolamrt] Jul 25, 2013

I am just thinking about all the implications and it's awesome. Those companies offering backup disk drive services to "the cloud" cannot guarantee that Uncle Sam hasn't grabbed the data as it's moving over. Companies promoting cloud based solutions, like Microsoft and their new Office Product, must be sweating big bullets right now. Go ahead Jack in the Box and put your secret sauce recipe on a spreadsheet in what you think is a safe cloud based solution and see how quickly some larcenous fed sells it to a competitor.

The world is no longer a safe place for business to operate. Everyone needs to go back to hard bound ledgers and quill pens. Corporate America had better be paying attention.

No wonder Obama wants to talk about anything else but this.

/ 4like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@carolamrt [http://www.cnet.com/profile/carolamrt] Why would they be sweating? Their TOSs & AUPs all warned you they would give the fuzz whatever they wanted on request.

As for business, if some low-level analyst were to steal and sell their secret sauce recipe, think of what would happen: a large, quiet donation to the party in the White House, some forensic auditing, some analyst going to jail for economic espionage for ten years. Remember, big business is one of the USA's designated winners. They

won't be allowed to lose, no matter how many polite mulligans it takes.

/ **like []reply []**

Lerianis6 [http://www.cnet.com/profile/Lerianis6] Jul 25, 2013

Those TOS's and AUP's are in violation of various federal, state and local laws. I.E. they aren't worth the electrons they are displayed on your screen with. No, they do that to TRY to cover their butts and usually people are too feeble to challenge them because they bellow about "You signed a ToS!"

/ **like []reply []**

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

im just think outside the box here. Lets assume that we can't stop the prying, so instead we set up automatic streams of emails i.e. every day my pc sends 200 emails to all my contacts, but on the other end I have already told the intended recipient exactly what time the relevant email was sent with date/time stamp. So they know which one is good and which ones are trash. Kind o f a blade of grass in grass scenario. Confusing for user = impossible for onlookers

(I guess you would have to set up an auto trash bot as well) But the information would be too overwhelming to possibly read through and find anything relevant to prying eyes.

/ 1**like []reply []**

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

What if we do both Start using the spam concept and encrypted files, Would that Bog the NSA computers down?

/ like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@JOESTMANN [http://www.cnet.com/profile/JOESTMANN] The NSA is authorized by law to keep messages suspected of having a hidden meaning essentially forever. So Moore's Law and black budgets will eventually catch up to you; it's only a question of whether the information in the hidden message would still be actionable or not.

It's also a question of what email provider would allow you to send 200 messages per day to every one of your contacts on an ongoing basis, and whether your recipients' email providers would take such a presentation as a flooding attempt or broken spam relay and work their way back to you, possibly terminating service.

Further, most fuzzing can be easily distinguished from actual signal based on speaker identification. Even when trying to conceal their writing style, the form and structure of a person's writing will show traits that are hard for a writer to conceal but easy for a computer to measure.

Besides, if your correspondent is using a PRISM-enabled mail host, a live feed of mailbox actions may be available. An analyst could simply tell the matrix "more like this please", and the noise will start to fall off.

/ 1like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv [http://www.cnet.com/profile/marxmarv] @JOESTMANN [http://www.cnet.com/profile/JOESTMANN] I see so once the cats out of the bag GG.

/ like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@JOESTMANN only saying that more hay isn't a very effective countermeasure

against *content* surveillance. It can be useful against *metadata* surveillance but only under very limited circumstances (ruses like presenting poor opsec or joining online ballot-stuffing actions, or hiding a very small amount of information within each message that only your recipient can detect and reassemble).

/ like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv @JOESTMANN I had this epiphany once years ago, that if The Govt. wanted to start a cold target investigation the best place to start was not with the people using net com more, but with the people who weren't using it very often but could. which lead to my initial out of box idea, but it would only cause problems not create solutions I guess.

/ like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Good, good, you're thinkin' like the predator. That's essential. But with all that input data, starting from zero will only take one down the rabbit hole. As I understand it, current practice is to start with a known real-world point of contact (an email address, phone number, other identifying information), map it onto the matrix to find people who resemble that identifying info from the inside of the glass (not exact, remember, this is dirty, unstructured data), find their associates of interest from inside the glass, and if anyone or anything looks like probable cause, pass it over to the FISA court, get the warrant back and go to step 1.

Ed Snowden suggested in an interview a few months back that encryption is probably still safe, but that endpoint security was a joke. That is, it's much easier for them to put a keylogger or rootkit or whatever in your PC than to crack your key, if they think you might be worth it.

/ like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv @JOESTMANN But if all the data is from unknown sources what basis is there to start an investigation to begin with, The only way it would work is if the system had time to develop a history of data. to be useful in the future! Thats why they were only mapping net com metadata, it wasnt to spy per say but to create a data base of "leads" You could encrypt all you wanted, that still wouldn't effect there system matrix from doing what its designed to do. Shady..

From my perspective I think it is an acceptable. The Govt. PR Dept. Sucks!

/ like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

I do feel awkwardly smug, not only was my epiphany plausible the NSA actually built a system to test it. "Local Artist imagines Govt. Spy matrix"
From my perspective I think it is an acceptable use of tech. And the Govt. should have been more forthright. The Govt's PR Dept. Sucks!

/ like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv [http://www.cnet.com/profile/marxmarv] @JOESTMANN [http://www.cnet.com/profile/JOESTMANN] So I guess the reason the NSA is probing Microsoft is to get an access code or have one installed in Systems prior to leaving factory, for remote access of said suspects systems. Didnt China come up with that idea.

/ like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@JOESTMANN [http://www.cnet.com/profile/JOESTMANN] But it's not from unknown sources. Remember the leaked Verizon order? (Incidentally, call detail records were one of the items requested, but there are many different surveillance programs, with one or many sources each.) Business records were one of the items Verizon and presumably others were required to turn over. The subscriber identities included in these business records would provide an easy and reliable (since the telco's money is at stake) dictionary to translate identities between the virtual world and the real world. Perhaps such a dictionary might not be very complete, and traditional methods might be called in to help in identification of a person of enough interest but .

It gets even more interesting when you add the dimension of time and assume that temporal clustering suggests causality. Say, for example, a guy receives a call from a person of interest, then places calls to a few other people within a certain period of time. Those people called are now of higher interest than they were before, and likewise your other contacts are now of lesser interest.

I too think it's unacceptable from any standpoint, but I also believe it's important to understand well the capabilities of systems if one wishes to exert influence within or upon them. That usually means piecing together hundreds or thousands of tweets, forum posts, blog posts and comments and other sources, filtered through a lifelong interest in and fascination with computing systems and maybe having read The Art of War once or twice many moons ago. Of course, working without leaked classified information is merely speculation, but one can at least strive to speculate responsibly (and remember not to drive afterward).

/ **like []reply []**

OldHippieEnt [http://www.cnet.com/profile/OldHippieEnt] Jul 25, 2013

Even the newest newbie must understand, apart from the obvious civil liberties implications, that this could totally compromise every single e-commerce transaction.

Is the government truly insane enough to destroy e-commerce for its own selfish ends?

/ 1like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@OldHippieEnt [http://www.cnet.com/profile/OldHippieEnt] Its more specified than that. Its the executive branch of the govt. And yes they could unwittingly change everything for the worse. The president doesn't want to give back the Power of the Patriot Act , and the united states will be in an continuous war to justify the control of the Patriot act. If we don't strike down the power of the Patriot act, we could very well be looking at the turning point in US history.

/ 1like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@OldHippieEnt [http://www.cnet.com/profile/OldHippieEnt] Well, you saw what they did for the health insurance industry: people won't buy insurers' defective-by-design products? Mandate that transaction and levy fines on those who don't.

/ like []reply []

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv [http://www.cnet.com/profile/marxmarv] @OldHippieEnt [http://www.cnet.com/profile/OldHippieEnt] Whats funny is that Obama and Romney both wanted Citizens United to suceed, and now Companys are bringing a class action suit against the Govt. using Citizens United to protest the health care bill.

/ like []reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@JOESTMANN [http://www.cnet.com/profile/JOESTMANN] **@OldHippieEnt [http://www.cnet.com/profile/OldHippieEnt]** Not the whole thing... if you think that's funny, what's hilarious is that almost all of the ACA has been pushed back, but only the individual mandate will begin on schedule, ready or (more likely) not. That suggests that the rent stream for insurers was the motivation for this law and health insurance was the wooden nickel with which to buy popular assent.

/ **like []reply []**

JOESTMANN [http://www.cnet.com/profile/JOESTMANN] Jul 25, 2013

@marxmarv @JOESTMANN @OldHippieEnt Thats not funny, if what your saying ends up being true, Company s could wash there hands of providing health insurance b/c now the Govt. is forcing individuals to pay or pay us. Your probably right tough, this whole thing was just a money grab by The President. Id better start an investment portfolio Insurance co. are going to be too big to fail.

/ **like []reply []**

Lerianis6 [http://www.cnet.com/profile/Lerianis6] Jul 25, 2013

@marxmarv [http://www.cnet.com/profile/marxmarv]

How are they 'defective by design', marxmarv or are you just shooting out of your posterior there?
Health insurance is a very good thing. It's meant to allow people to go to doctors and use the massive power of multiple people to negotiate with doctors and hospitals to lower their prices to a reasonable level.
In fact, if we wanted to fix things totally on the health care front, we would allow people to buy into Medicare (with perhaps differing coverage levels like private insurance and different deductibles like private insurance).

/ **like []reply []**

Looking2bpleased [http://www.cnet.com/profile/Looking2bpleased]
Jul 25, 2013

@Lerianis6 [http://www.cnet.com/profile/Lerianis6]

@marxmarv [http://www.cnet.com/profile/marxmarv]

@Lerianis6 [http://www.cnet.com/profile/Lerianis6] **@marxmarv [http://www.cnet.com/profile/marxmarv]** Reading this chain of posts, I must admit I like the thinking process being applied here by most posters. However @Lerianis6, I take umbrage to your trite response. Have you looked at the coverage?

"Health insurance is a very good thing"... hard to argue your non-relative point. You mention allowing people to buy into Medicare, and then equate that to private insurance. I don't know how you'd mix up so much non-info information into your response to the original poster.

The government has mandated insurance, and fines the end user (citizen) for non-participation. That's so true of this 'Health Care Program' that you can not effectively defend it.

O.K., I'll make general statements: "We all need health care." "We are all willing to pay our part (or as much as we can)". Which statement is more true? That's the crux of the issue here, and the government would rather mandate a 'tax' (which is what it is), then work on any real long term solutions.

Anyway, you destroyed your own argument with the words 'like private insurance' - that is what it has been for a long time, and it was more or less successful, along with Medicare.

But it's time to face the reality of the Baby Boomers (that's me), and the reality that a real discussion needs to occur, not lip service, and not socialized medicine, and certainly not 'taxation without representation'.

Our executive branch has overreached into our pockets once more, and it won't be the last time. They are incapable of rational thought, unless of course it is near election time - then they start to really work on their agenda - mainly getting reelected.

/ like []reply []

Lerianis6 [http://www.cnet.com/profile/Lerianis6] Jul 25, 2013

@Looking2bpleased [http://www.cnet.com/profile/Looking2bpleased]

I take umbrage at YOUR post, which FAILS TO REALIZE that the government FINES US FOR NOT DOING A LOT OF STUFF. Especially when not doing that (even when it is buying a service... cough..... auto insurance) is damaging to the populace at large.

It's past time to realize that in the real world, you cannot live without health insurance of some form. You just cannot, it's impossible to live without it unless you want to be stress yourself into an early damned grave about "What if I get injured!?" on a daily basis.

No, mandating that everyone has to have health insurance will improve things by:

1. Giving a bigger pool for insurance companies to draw from, thereby diluting the old "ONLY THE SICK BUY INSURANCE" BS argument that they have been trying to foist on us for years.

2. Getting people to primary care physicians where their ills can be treated BEFORE they need expensive hospitalization or, if they do need hospitalization even after that primary care, at a point where it's easier to treat them in the hospital and much less expensive.

No, simply put, the old "IF YOU'RE YOUNG, YOU DON'T NEED HEALTH INSURANCE!" idiocy needs to go bye-bye forever. I've had insurance since I was still in my MOTHER'S WOMB and was paying 500 dollars a month for a platinum plan until very recently.

Sure, I make 60K a year, but I've also gone to a plan that costs less than 120 dollars a month and if I had two children, would only cost 60 bucks more per month to insure them!

Plus, most common things (vaccinations, a yearly health checkup, dental visits) are free with that insurance! Which those are basically the only thing I use my health insurance for, besides the occasional ear infection.

/ like []reply []

linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior] Jul 25, 2013

HTTPSeverywhere from EFF in every Firefox download combined with easy installation of PFS in every Apache download would lay the issue to rest forever.

Whether you're a Pirate or a Libertarian, this intrusion is simply unnacceptable. Encrypt /everything/ by default. Vote Pirate at the next election.* Educate your friends. Your family. They want a war on privacy? We'll give 'em a war all right: with complete and overwhelming defence.

Visit encrypteverything.ca - a Pirate Party of Canada Project to DEFEND YOURSELF

* Not that it helps with unnaccountable Election Machines.,

/ 1 like [] reply []

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior] Did you come here from /.? RTFA! HTTPS Everywhere won't do you a lick of good if an eavesdropper has the server's private key, which given the state of IT security today wouldn't be terribly hard to get at all, even easier if one were in the habit of buying 0day exploits from shady foreigners (which the NSA are).

/ 1 like [] reply []

linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior] Jul 25, 2013

@marxmarv [http://www.cnet.com/profile/marxmarv] @linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior] What HTTPSeverywhere does is includes the SSL observatory, which ensures that "Google Inc", which you see, is the "Google Inc" that others see, thwarting wiretaps.

Also, non-CA issued certs AKA Self-signed are pretty secure. Kick EH!

/ like []reply []

Lerianis6 [http://www.cnet.com/profile/Lerianis6] Jul 25, 2013

@linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior]

Until they threaten to throw that person who knows the 'self-signed' key into prison, it's secure. Most people will cave like a tissue paper castle that has had an elephant sneeze on it in that position.

/ like []reply []

noreg [http://www.cnet.com/profile/noreg] Jul 25, 2013

@linuxroadwarrior [http://www.cnet.com/profile/linuxroadwarrior] So the solution to the government being able to read your encrypted data is … to use the form of encryption they have the key to already? How does that help?

/ like []reply []

noreg [http://www.cnet.com/profile/noreg] Jul 24, 2013

"But when asked whether Microsoft would turn over a master key used for Web encryption or **server-to-server e-mail encryption [http://news.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."

I don't believe this for a minute. Even if the government said "Do this, or we arrest you", as they apparently have in the very recent past? Is Microsoft actually claiming that their executives or other employees would go to prison over this issue rather than turn over the keys? If compelled, would they shut down all their online services (and risk legal repercussions) by destroying the keys, rather than supplying them to the government?

And even if we were to believe that Microsoft would not in any circumstance turn over the keys, why are they drawing the line at SSL keys, and not any of the other

data they've been asked to secretly provide to the NSA? Where exactly is their line?

Have they (or any other company) ever done anything even remotely similar to this in the past? Why should we believe this? Isn't it a bit convenient that they seem to have drawn a line exactly at "SSL private keys", the hot issue of the day? Why didn't they offer such assurances when being asked by the NSA to *circumvent* encryption, as they did over the past year with Outlook.com, SkyDrive, and Hotmail?

Come to think of it, is this just a clever way to dodge the specific question being asked? One of the leaked NSA documents says: "For Prism collection against Hotmail, Live, and Outlook.com emails will be unaffected because Prism collects this data prior to encryption". Maybe Microsoft won't bother providing SSL private keys because they prefer to just offer the raw data to the NSA.

I don't mean to pick on Microsoft specifically. I'm sure all of the big companies involved (and also the NSA) are doing exactly the same thing. They're all completely full of shit.

/ 2**like []reply []**

marxmarv [http://www.cnet.com/profile/marxmarv] Jul 25, 2013

@noreg BIngo. They can't see a circumstance in which they would provide it, because they'd rather just let the NSA install a black box behind the firewall where the unencrypted data flows and make uneasy but reassuring noises in the press.

But to answer your question, forged SSL certificates have been created and used to spy on dissidents, particularly in Iran (and if they can do it all low-tech, surely the NSA can do it one better). For example, see **http://www.computerworld.com/s/article/9219731/Hackers_spied_on_300_000_Iranians_using_fake_Google_certificate [http://www.computerworld.com/s/article/9219731/Hackers_spied_on_300_000_Iranians_using_fake_Google_certificate]**

/ 2**like []reply []**

WasteLayer [http://www.cnet.com/profile/WasteLayer] Jul 24, 2013

What annoys me the most is the fact that the government uses the ever-expanding umbrella of "terrorism" to justify this nonsense.

US Citizens did not create terrorism, ridiculously intrusive and invasive US foreign policy did. Our leaders created terrorism by spying and manipulating foreign governments to the point that citizens of those nations are now prepared to wage war against the US in response to these policies.

So our governments response is to spy EVEN MORE, EVEN ON IT'S OWN CITIZENS, in the name of "terrorism"?

How about this... Leave EVERYONE alone. Many things will suddenly become much, much better. We'll have so much cash and free time on our hands that we'll no longer need to worry about oil and "forward-deployed" forces.

/ 8**like []reply []**

purplecheeseslice [http://www.cnet.com/profile/purplecheeseslice]
Aug 2, 2013

@WasteLayer [http://www.cnet.com/profile/WasteLayer] YES.

/ **like []reply []**

Show More Comments

Add Your Comment [#postComments]