MUST READ HOW TO INSTALL LINUX MINT ON YOUR WINDOWS PC

NSA chief: Encryption isn't bad, it's the future

...but intelligence agency still wants access to encrypted communications.

By Steve Ranger | May 28, 2015 -- 07:15 GMT (08:15 BST) | Topic: Security

Image: Siim Teder/Estonian Defence Forces

The director of the US' National Security Agency has said that encryption is not a bad thing - but that the authorities still need to be able to gain access to encrypted communications to protect the country's citizens.

Speaking at a cyberwarfare (http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/)

conference in Estonia on Wednesday, admiral Mike Rogers, director of the US National Security Agency and head of US Cyber Command, said: "You're not going to hear me say that encryption is a bad thing. I don't think it is a bad thing. Encryption is not bad. Encryption is a fundamental part of the future; I think it would be ridiculous to pretend otherwise."

However, he said that it is a challenge to ensure the security of US citizens and protect their right to privacy at the same time. "It's not either or in the United States - we have to do both." The question is how to create a legal framework to do both, he added.

"Can we create some mechanism where within this legal framework there's a means to access information that directly relates to the security of our respective nations, even as at the same time we are mindful we have got to protect the rights of our individual citizens?"

Encryption is a hot topic right now (http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/): following the revelations by NSA-contractor-turned-whistleblower Edward Snowden about the scale of internet surveillance by the intelligence agency, many more companies have started encrypting their customers' communications.

However, the growth in such communications has in turn led to fears from intelligence agencies and law enforcement - particularly in the US and UK - that, by using uncrackable encrypted communications, criminals will be able to plot in secret. As a result, a number of politicians and law enforcement chiefs want companies to be obliged to unscramble customers' communications when requested by authorities.

READ THIS

(http://www.zdnet.com/article/encryption-for-everyone-the-free-easy-to-use-service-that-wants-to-change-how-you-think-about/)

Encryption for Everyone: The free service that will change how you think about security (http://www.zdnet.com/article/encryption-for-everyone-the-free-easy-to-use-service-that-wants-to-change-how-you-think-about/)

For most people, encryption is seen as too hard to use, a bit niche, or something for the 'tin foil hat' brigade. A German project's hoping to change all that.

Read More (http://www.zdnet.com/article/encryption-for-everyone-the-free-easy-to-use-service-that-wants-to-change-how-you-think-

about/)

Privacy campaigners argue that the use of encrypted communications is a right and that creating any backdoor into encryption systems would fundamentally undermine their security.

Rogers said a framework to allow law enforcement agencies to gain access to communications is in place within the phone system in the United States and other areas, so "why can't we create a similar kind of framework within the internet and the digital age?"

He added: "I certainly have great respect for those that would argue that they most important thing is to ensure the privacy of our citizens and we shouldn't allow any means for the government to access information. I would argue that's not in the nation's best long term interest, that we've got to create some structure that should enable us to do that mindful that it has to be done in a legal way and mindful that it shouldn't be something arbitrary."

Speaking at the conference, organized by the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence thinktank, Rogers also said that rather than individual countries setting their own rules for control of the internet, international rules similar to those used to govern use of the world's seas should be established - a kind of maritime law of the internet.

"Can't we create a global commons that enables open reliable safe secure and resilient communications the flow of information and ideas that enables us to do it in a framework that maximizes its use for all of us?" he said.

Earlier this month China published a draft national security law (http://www.zdnet.com/article/china-tightens-cybersecurity-controls-to-limit-foreign-spying/) which in contrast asserts its "sovereignty" with regards to the internet and cybersecurity.

More on encryption

- The undercover war on your internet secrets: How online surveillance cracked our trust in the web (http://www.techrepublic.com/article/the-undercover-war-on-your-internet-secrets-how-online-surveillance-cracked-our-trust-in-the-web/)
- Inside the secret digital arms race: Facing the threat of a global cyberwar

(http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/)

- The impossible task of counting up the world's cyber armies (http://www.zdnet.com/article/counting-up-the-worlds-cyber-armies/)
- Encryption: More and more companies use it, despite nasty tech headaches (http://www.zdnet.com/article/encryption-more-and-more-companies-use-it-despite-nasty-tech-headaches/)

Recommended For You

Promoted Links by Taboola

Perfectly legal ways you can still get Windows 7 cheap (or even free)

Windows Phone to close in on iPhone by 2017

JOIN DISCUSSION

SHOW COMMENTS

RECOMMENDED FOR YOU

Evaluating file sync and share solutions: 12 questions to ask about security (Norway)

White Papers provided by Dropbox

LEARN MORE

PGP co-founder: Ad companies are the biggest privacy problem today, not governments

The ad-blocker dispute is "going to be a lot of fun to watch," said Jon Callas.

By Zack Whittaker for Zero Day | February 4, 2016 -- 14:51 GMT (14:51 GMT) | Topic: Security

PGP co-founder Jon Callas. (Image: SkyDogCon via Twitter)

NEW YORK -- Ask one of the foremost cryptographers of the modern generation what the biggest privacy issue is today and you might expect something like backdoored encryption or government spying.

Jon Callas, co-founder of encryption software PGP ("Pretty Good Privacy"), who has worked at Apple, Entrust, and now Silent Circle, a security software maker and Blackphone maker, is probably best equipped as one of the best litmus tests on the "state of the security union" today. Speaking last week, a day ahead of Data Privacy Day (https://www.youtube.com/watch?v=uAJar-OeNlI&feature=youtu.be) where he gave a Reddit "Ask Me Anything" talk (https://www.reddit.com/r/IAmA/comments/434om8/hi_im_jon_callas_cryptographer_who_cofounded_pgp/), like many members of the security community, he was refreshingly blunt.

"I don't think we're doomed," Callas told me in a phone call last Wednesday. Reassuring as it was to hear that, he did warn of a brewing brouhaha on the horizon, one that doesn't involve government spying, hackers taking down websites, or data breaches that pilfer your private information.

"The adblocker dispute is going to become one of the fundamental battles on privacy," said Callas. "It's going to be a lot of fun to watch."

Think about the biggest tech companies going today: Apple, Facebook, Google, and Microsoft. These tech titans have more data on you than anyone or anything else out there -- even governments. (Why do you think they are served a near constant stream of warrants for user data?) In most cases, you serve up your data voluntarily, from emails to text messages, photos and documents, and social networking data.

But there's a growing divide between Silicon Valley companies about what they do with your data.

Advertising keeps most websites and services, like Google and Facebook, free to use. They can be annoying and intrusive, but they can also track which sites you visit across the internet and search terms you

READ THIS NEXT

(http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/)

Apple, in refusing backdoor access to data, may face fines
(http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/)

Analysis: Yahoo faced growing fines in 2007 when it refused to participate in the PRISM program, which sets a precedent for non-compliance with government demands.

Read More
(http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/)

enter. Ad networks collect information about you -- browsing habits, search results, and other demographic data (such as your age, location, and education) -- which they argue helps them serve better ads. Callas explained that the users of these ad-driven services aren't the customer, but are the product -- in that they supply the data that drives the ad business.

"You are not giving up your information, you're basically selling it," he said. "We now know that the main privacy issue is with the ad companies, not with the government," said Callas.

In the wake of the Edward Snowden disclosures, every tech company is pushing for greater security, better privacy, and more transparency. But increasingly, tech companies are becoming polarized.

You have Alphabet (which owns Google and YouTube) and Facebook making about 89 percent (http://www.zdnet.com/article/alphabet-google-q4-2015-earnings-revenue-cloud/) and about 95 percent (http://venturebeat.com/2015/11/04/facebook-beats-q3-2015-expectations-with-4-5b-in-revenue-and-an-eps-of-0-57/) of revenue respectively. Yet, compare that to companies that don't really need your data to make money, but aim to put privacy at the top of their customers' agenda. Microsoft's ad revenue is a fraction (https://www.microsoft.com/investor/EarningsAndFinancials/Earnings/PressReleaseAndWebcast/FY16/Q2/de of its overall quarterly revenue compared to its behemothic cloud and enterprise units. Apple makes the vast majority of its money from mobile device and desktop sales.

"The adblocker dispute runs right into this," said Callas. Everyone is trying to get on the privacy bandwagon; companies that don't sell on your data are the most prepared if the ad industry takes a downturn.

"The irony is that we have this line where you have Apple and Microsoft on one side, and then you have Google and Facebook," said Callas. "We're caught between these two groups of companies through our buying habits and reading habits and other things affect what they're doing."

Apple and Microsoft store data in-house to make their products better, and isn't sold onto third-parties. The financial downside is that you have to buy into their products and services, often up front, in order to enjoy the privacy that they provide. Apple, for example, provides perhaps the world's biggest end-to-end encrypted messaging service that has riled governments for shutting them out, but an entry level compatible device will still set you back a few hundred dollars.

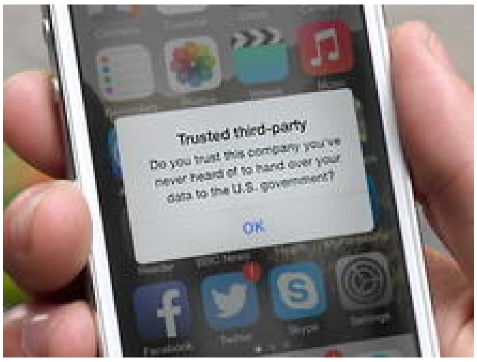
It's the price you pay for privacy.

The bizarre dichotomy is that companies like Google and Facebook, which collect, store, and sell your data to make money, are "desperately" edging away from these models with other business interests, Callas said. As the ad-blocker dispute rolls on, these businesses will suffer decreased revenues, and face having to deviate and transform their business models away from ads.

And the ad-blocker dispute isn't going away any time soon. Many find ads to be intrusive, so they install third-party browser plugins to prevent them from showing. Others are more privacy minded, and want to prevent being tracked across the internet.

Just last week, Randall Rothenberg, a chief executive of a non-profit trade group which represents advertising companies, accused ad-blocking companies (http://www.wsj.com/articles/iab-ceo-continues-to-hammer-ad-blockers-1453849338) of being "self-proclaimed libertarians whose liberty involves denying freedom to everyone else" and "an old-fashioned extortion racket."

EXCLUSIVE


Trusted third-party
Do you trust this company you've never heard of to hand over your data to the U.S. government?
OK

(http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/)

Meet the shadowy tech brokers that deliver your data to the NSA
(http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/)

These "trusted third-parties" may be the most important tech companies you've never heard of.

Read More
(http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/)

Rothenberg said publishers were set to lose close to $22 billion in 2015 because of ad-blocking, a jump of 41 percent. Companies like Facebook and Google face the prospect of adapting their business models, or suffering massive revenue losses.

"The ad people are absolutely right in that their business models aren't going to work when there are no advertisements," said Callas.

READ MORE

Why the CIA wanting encryption backdoors is a failure of leadership, not intelligence (http://www.zdnet.com/article/cia-encryption-backdoors-a-failure-of-leadership-not-intelligence/)

Apple, in refusing backdoor access to data, may face fines (http://www.zdnet.com/article/apple-in-refusing-backdoor-access-to-data-faces-huge-fines/)

NSA is so overwhelmed with data, it's no longer effective, says whistleblower (http://www.zdnet.com/article/nsa-whistleblower-overwhelmed-with-data-ineffective/)

As the Snowden leaks began, there was "fear and panic" in Congress (http://www.zdnet.com/article/snowden-leaks-fear-and-panic-in-congress/)

How Microsoft's data case could unravel the US tech industry (http://www.zdnet.com/article/why-microsoft-data-case-could-unravel-the-us-tech-industry/)

If you have 'nothing to hide', here's where to send your passwords (http://www.zdnet.com/article/if-you-have-nothing-to-hide-heres-where-to-send-your-passwords/)

Meet the shadowy tech brokers that deliver your data to the NSA (http://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa/)

JOIN DISCUSSION