NSA chief seeks compromise on encrypted phone snooping

February 23 2015, by Rob Lever

National Security Agency Director Adm. Mike Rogers speaks about cyber security at The New America Fondations cyber security conference at the Ronald Reagan building February 23, 2015, in Washington, DC

The National Security Agency chief pressed on Monday for a compromise which allows intelligence services to snoop on encrypted devices to combat terrorism, within a "legal framework" to protect user

rights.

Admiral Michael Rogers told a Washington cybersecurity forum that he does not believe Americans should be divided on the issue of encryption—which makes it nearly impossible for outside parties to gain access, even in some cases with a warrant.

Rogers endorsed the view expressed by FBI director James Comey on gaining access to encrypted mobile devices as necessary for law enforcement.

Comey last year warned that law enforcement could be hampered in critical investigations after Apple and Google said they would encrypt their smartphones and give users the keys, making it impossible to hand over data even with a court order.

"Most of the debate I've seen is that it's either all or nothing, that it's either total encryption or no encryption at all," Rogers said.

Rogers said it should be feasible to "come up with a legal framework that enables us within some quasi-process to address... valid concerns if I have indications to believe that this phone, that this path is being used for criminal, or in my case, foreign intelligence or national security issues."

The NSA chief called for the same kind of cooperation used to fight child pornography and exploitation, where tech firms report potential criminals to authorities.

"We have shown in other areas that through both technology and a legal framework and a social compact that we can take on tough issues, and I hope we can do the same thing here," he said.

Regaining trust

Rogers said the NSA needs to be able to carry out its mission as well as regain trust of the American public.

"This simplistic characterization that one side is good and one side is bad is a terrible place for us to be as a nation. We have got to come to grips with some really hard fundamental questions."

The NSA has come under intense scrutiny both at home and abroad after former contractor Edward Snowden leaked documents about government surveillance programs that sweep up vast amounts of data from Internet and phone communications.

Rogers declined to comment on the latest reports from last week that the NSA implanted spyware on commercially made hard drives, and that it worked with British intelligence to hack into the world's biggest maker of SIM cards to be able to access mobile communications.

"We fully comply with the law," Rogers said. "We do that foreign intelligence mission operating within (a legal) framework."

But Rogers appeared to have a hard time persuading some in the audience who argued that giving encryption keys to the NSA would weaken security and could force US firms to give the same access to foreign governments.

Alex Stamos, the chief information security officer for Yahoo, asked Rogers whether "we should be building defects into the encryption in our products," saying these would be "backdoors or golden master keys for the US government."

Rogers said he disliked the term "backdoor," saying it should be a

transparent mechanism with legal supervision.

Bruce Schneier, chief technology officer at the security firm Resilient Systems said the government request for access reprises an effort by the US in the 1990s to gain access to Internet encryption keys.

The effort was abandoned in the face of opposition from tech firms.

Whether it is software or hardware, Schneier told AFP, "nobody would want this. Someone in France is not going to buy something if there is a framework for (NSA) access."

Citation: NSA chief seeks compromise on encrypted phone snooping (2015, February 23) retrieved 27 April 2024 from https://phys.org/news/2015-02-nsa-chief-compromise-encrypted-snooping.html