The Christian Science Monitor

Influencers: Stronger encryption on consumer devices won't hurt national security

The vast majority of Passcode Influencers oppose weakening encryption so that law enforcement could have easier access to personal data. In fact, many say that stronger privacy protections will ultimately improve national security.

Sara Sorcher

March 11, 2015

Three-quarters of Passcode's Influencers disagree with FBI Director James Comey, insisting stronger encryption on consumer devices would not hinder law enforcement and intelligence agencies so much that it would harm national security.

"It's crucial that users demand the highest level of security to both protect our personal privacy and mitigate the potential harm that can result from theft of personal data. Unquestionably, encrypting the content of smartphones makes it more difficult to access that information; that's the point," said Nuala O'Connor, head of the Center for Democracy and Technology. "However, there are still many legal channels police can pursue to access encrypted data."

Mr. Comey and intelligence officials have criticized companies such as Google and Apple for strengthening encryption on consumer devices because they say it will stymie law enforcement as they track criminals and terrorists. While the 73 percent of Influencers largely acknowledged that encryption will occasionally pose some obstacles to law enforcement, they insisted they were not severe enough to justify built-in government access to data.

"Evidence that this is a serious problem demanding a policy response is laughably weak," said Cato Institute senior fellow Julian Sanchez.

"We live in a Golden Age of Surveillance. Never in human history have police had such easy access to such vast quantities of data about people. They'll still be able to use subpoenas or court orders (and the threat of contempt penalties or even obstruction charges) to compel people to decrypt data; they can still surreptitiously attempt to get people's passphrases through physical surveillance," Mr. Sanchez continued. "It is flat out insane to suggest that we should undermine the security of a technology used by hundreds of millions

of people for legitimate purposes because of the minuscule fraction of cases where crypto will be the make-or-break factor in a legitimate investigation."

Security pros also had objections, taking issue with intelligence officials' assertions that it would be technologically feasible to provide government access to encrypted data through a secure channel without compromising users' security.

"Much greater harms to national security would result from the government deliberately weakening encryption protocols (again) as the FREAK vulnerability demonstrated this past week," said Chris Finan, chief executive officer of Manifold Security. "DC policymakers shouldn't seek a middle-ground solution on this issue, because it simply doesn't exist when it comes to cryptography.

"The only answer is to support the strongest possible encryption protocols, while also enabling law enforcement professionals with the resources needed to conduct classic police work," Mr. Finan continued. "The FBI director should realize that the days of relying on backdoor technology shortcuts are over. Encryption is as empowering a technology as gunpowder or firearms, policymakers need to appreciate the irreversibility of this paradigm shift and adapt. Quite simply, governments no longer enjoy a monopoly on technologies like cryptographic protocols or offensive cyberwarfare exploits. There are no tech magic bullets to address these policy challenges."

The Passcode Influencers Poll brings together a diverse group of more than 80 security and privacy experts from across government, the private sector, academia, and the privacy community. To preserve the candor of their responses, Influencers have the choice to keep their comments anonymous, or voice their opinions on the record.

"While it may make it harder for the government to protect us, I see no difference between this and a file locked in a cabinet in my house," said one Influencer who chose to remain anonymous. "This to me is a Fourth Amendment issue."

Comey did have some backing among 27 percent of Influencers. "We need government and industry to work together on a solution that protects our nation through lawful intercept and ensures civil liberties and privacy," said (ret.) Gen. Keith Alexander, chief executive officer of IronNet Cybersecurity and former National Security Agency director.

Robust encryption, another Influencer added, "is important to protect American’s privacy and to protect our infrastructure from cyberattacks. But encryption that allows criminals or terrorists to operate with impunity beyond the reach of lawful process would threaten our national security. There must be a balance between the two."

This idea, another Influencer said, "is nothing short of revolutionary in that it challenges the very premises of the Fourth Amendment. Privacy has always been central to our Republic but it has also always been circumscribed via balanced rules, execution, and oversight by our three branches of government. Encryption without any state access eliminates this well-worn historical (and Constitutional) approach."

Who are the Passcode Influencers?

For a full list, check out our interactive masthead here.

Comments: No

"US citizens' right to privacy would be jeopardized by promoting weak or no encryption on consumer devices. Instead, law enforcement agencies should find other ways to make their case against a suspect or intelligence target."**– Jeffrey Carr, Taia Global**

"Stronger encryption is a given; it is going to happen. And, so are efforts by law enforcement and intelligence agencies to collect data regardless. If we believe there are circumstances in which it is legitimate for authorities to do so, and I do, then we need to propose alternative means. 'Just say no' to backdoors is not enough." **– Steve Weber, UC Berkeley**

"Strong encryption exists and bad guys will always know how to find it. All such restrictions will do is limit honest people's access to the protection that encryption brings. Besides, we've never conditioned people's rights to privacy, free speech of to live a free life on the preferences of law enforcement." **– Cindy Cohn, Electronic Frontier Foundation**

"Encrypting smartphones and other tech products will help protect against malicious hacking, identity theft, phone theft, and other crimes. By choosing to encrypt popular operating systems by default, companies are making this security feature easier to use and more accessible to regular smartphone users who do not seek out increased security protection. This will reduce overall crime by protecting all smartphone users, rather than just those who are already security-conscious. Products and software with strong encryption have been freely available to the public – including criminals – for many years, and have not rendered law enforcement helpless to investigate crimes. The digital revolution has made more data about us available than ever before, and the government has more tools to obtain and analyze that data than ever before. The volume of government surveillance increases almost every year. The claim that companies' adoption of strong encryption by default will suddenly lead to government "going dark" and unable to access critical information is speculative at this time." **– Harley Geiger, Center for Democracy and Technology**

"James Comey's argument that strong encryption on consumer devices would harm national security ignores the most important function of national security, which is to ensure that our

civil rights and privacy that lays the foundation for participatory democracy is protected at all costs. As Ben Franklin so wisely summed up, 'Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.' " – **Sascha Meinrath, X-Lab**

"The better question is: Would national security be harmed even more if our data isn't encrypted, and thus vulnerable to theft by hackers and foreign intelligence agencies?" – **Chris Soghoian, ACLU**

"Device encryption does not stop the collection of data in motion such as voice calls, voice mail, text messages, emails stored at the provider, app meta data, and so on. There is no degredation in traffic analysis. Unmentioned in this debate is the harm prevented by device encryption when a phone is stolen or illicitly accessed, as well as the competative advantage such a manufacturer may get in the international market." – **Jeff Moss, DEF CON Communications**

"Any discussion of the negative impacts of pervasive encryption on national security and crime must necessarily also include a discussion of the positive impacts through improved resistance of the populace and global infrastructure to unrelenting, ubiquitous attacks that occur every minute of every day. There can be no rational (or responsible) policy debate without acknowledging both sets of equities. While there may be adverse impacts to certain law enforcement and government security activities that result from the pervasive use of strong encryption technologies, there are also positive impacts in the same domains. These same technologies assist the populace in defending their personal, corporate and private infrastructure against criminals, fraudsters, and would-be nation-state attackers." – **Bob Stratton, Mach 37**

"The public good is best served by strong encryption with no "back doors" for governments or corporations to exploit. Nothing has changed since this same issue was addressed in the mid-1990s when the Electronic Frontier Foundation won a landmark case in which U.S. courts determined that such code is free speech protected under the First Amendment." – **Janna Anderson, Elon University**

"Law enforcement's ability to trivially break encryption may sometimes have consequences on specific cases, but it's arguable that the mobile smart phone has become the 'personal papers' platform of this era. The Fourth Amendment to the US Constitution specifically states the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." – **Influencer**

"Not so much to be unmanageable." – **Influencer**

“A qualified ‘No” because while it may make law enforcement’s job more difficult, I think it’s the wrong question. For the past 20 years, those of us in the information security

business have been evangelizing for better security to protect the critical infrastructure in our Nation's public and private sectors that is responsible for the economic growth of our country. Taking a position that says technology has advanced so far that it puts national security at risk is a terrible argument. Dumbing down security and shunning the tremendous advantages of the advances in technology to make law enforcement's job easier is a 'head in the sand' approach that doesn't make sense. Even if it would work (which it wouldn't because bad guys will always find a way to circumvent technical controls), it doesn't make sense to try and put a governor on the throttle of technology. Suppressing the use of security technology simply makes the bad guys' job easier and the security professional's job harder. I understand how it makes the job of law enforcement and the intelligence community more difficult, but that's why the legal system has an entire branch of the U.S. Federal government dedicated to it." **– Mark Weatherford, Chertoff Group**

"While I respect the need for law enforcement to prosecute cases, we cannot facilitate local government access to personal data in the US, while criticizing foreign government access to personal data overseas (e.g., in China). I prefer targeted access as described in Steven Bellovin's 'Going Bright' paper." **– Richard Bejtlich, Fireye**

"Strong encryption is the classic double-edged sword. Actors seeking to harm US interests may use encryption to shield their activities from law enforcement and national security authorities, but it also protects US government and corporate data and communications from the prying eyes of foreign spies." **– Melanie Teplinsky, American University**

"Strong encryption is already in use by cyber criminals/terrorists that are real threats. It belongs on corporate and consumer devices to protect confidential information and individual privacy." **– Anup Ghosh, Invincea**

"The question is not simply whether it harms national security – it's whether any plausible way of compelling encryption with a back door is grievously harmful to the Internet ecosystem. (It is.) I wrote at length on this." **– Jonathan Zittrain, Harvard**

"It is not that simple. Strong security is critical to both short term and long term national security interests." **– Influencer**

"If we consider the protection of private sector intellectual property and citizen privacy to be critical elements of national security, prohibiting stronger encryption does more harm to our national security than allowing it. If the FBI wants to make an effective case, it needs to explain why its definition of national security trumps a broader definition that considers the privacy of our citizens to be a precious inalienable right." **– Rick Gordon, Mach 37**

"We are the midst of a crisis of insecurity. Data is leaking everywhere. We need manufacturers to be confident they not only can build secure systems, but that they will be allowed to." **– Dan Kaminsky, White Ops**

"We are not safer if the government can undermine our security. The problem is that Comey's back doors would allow *anyone* to undermine our security." **– Influencer**

"Intelligence agency and law enforcement access to information needed for national security purposes should, to some extent, include deliberation with and justification to companies that provide consumer products to (1) address issues of national security at a more minute and targeted manner and (2) to ensure that an acceptable level of an individual's right to privacy is upheld." **– Amy Chang, Center for a New American Security**

Comments: Yes

"But that does not mean that I think we should not have stronger encryption. We should never abdicate our right to personal privacy just to make it easier for Law Enforcement." **– Rick Howard, Palo Alto Networks**

"Greater encryption would invariably lead government agencies to engage in more supply chain attacks and other more intrusive measures that would be needed to obtain data from court authorized surveillance." **– Influencer**

"We – industry, government – should not start an encryption/anti-encryption arms race." **– Influencer**

"To be brusque, true but irrelevant. We understand and tolerate thousands of deaths due to automobiles. We understand and tolerate thousands of deaths due to firearms. We understand and tolerate thousands of deaths due to lifestyle. The question, therefore, is whether we are able to understand and tolerate thousands of deaths due to widespread strong crypto. If the answer is that we will not tolerate it, then unlike automobiles, firearms, and lifestyle we will, and must, move to prevent the availability of strong cryptography such that the number of deaths due to strong cryptography is absolutely de minimus compared to the number of deaths due to automobiles, firearms, and lifestyle. The difference, of course, is that because we have not centralized the control of automobiles, firearms, nor lifestyle there is no locus of political angst and anger over some sort of administrative failure at The Core. The very fact that we *have* centralized the control of cryptography is why there *does* exist a locus of political angst and anger, or there would be the minute a few thousand deaths could be attributed to some by-then-retrospective failure to have prevented the widespread deployment of strong cryptography. Even the bluest states could do well to re-read FDR's 1933 inaugural address (on fearing fear), which I quote at length with its progenitors as the invited essayist for the first issue of the Harvard National Security Journal." **– Dan Geer, In-Q-Tel**

"Yes, this is true but it is also the wrong question. More importantly is whether it harms national security enough that it is worth all the other costs. I believe that surely it does not. We need to prioritize a safe and secure Internet first and foremost. Compromises like this

hurt Americans, American companies, and ultimately the American economy. They undermine the US position with other countries, just as other national-security decisions, like those revealed to us by Snowden." **– Jay Healey, Atlantic Council**

"Robust encryption is important to protect American's privacy and to protect our infrastructure from cyberattacks. But encryption that allows criminals or terrorists to operate with impunity beyond the reach of lawful process would threaten our national security. There must be a balance between the two." **– Influencer**

"I agree subject to the caveat that if a mechanism existed that would guarantee law enforcement access under a court order, his concern would no longer be valid. The problem lies with the fact that with the current direction taken by manufacturers, there IS no such mechanism. Catastrophic from a law enforcement/intelligence point of view. And as such, from the national security point of view." **– Influencer**

"Whether that is a tradeoff that we should be willing to make is another question." **– Ely Kahn, Sqrrl**

"Will it harm national security? Yes. But this is a risk that our country might be willing to take." **– Influencer**

"But I don't know how much it will hurt. Conversely, it will help preserve privacy and security particularly in countries which do not enjoy the rule of law as we do in the United States. It should not be forgotten that almost all of our IT companies sell more overseas than at home." **– Influencer**