OPEN TECHNOLOGY INSTITUTE

Encryption Backdoors are a Dangerous Idea

And National Security and Intelligence Leaders Around the World Agree

Technical experts, civil liberties advocates, and internet companies have long urged that there is no such thing as a secure encryption "backdoor." Any mandate for companies to create a method for bypassing encryption in order to guarantee law enforcement could assess that information in a readable form would not only fail to address the problem law enforcement seeks to solve, it would render average internet users less secure. However, they are not the only ones warning against encryption backdoors. Current and former leaders of the national security and intelligence communities in the United States and abroad have been unequivocal: we must protect strong encryption, and backdoors are dangerous to national security, cybersecurity, and the global economy.

What follows is a collection of some of these leaders' remarks on the current encryption debate.

United States:

"Solid and technologically sound encryption systems are needed more than ever for data protection, data integrity, and confidentiality. At a time, for example, when voter databases are under assault from foreign actors, we need to be enhancing the integrity of our data systems, not reducing it. I have worked...to strengthen cyber protections, responded to breaches, and understand how difficult it is to build secure and resilient systems—introducing new vulnerabilities only exacerbates these challenges."

-**Robert Anderson**, former FBI Executive Assistant Director for Criminal, Cyber, Response and Services Branch (CCRSB), in an op-ed for The Hill in 2018.

"[W]e believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server, and enterprise level without building in means for government monitoring... Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security."

-**Mike McConnell**, former director of the National Security Agency and director of national intelligence; **Michael Chertoff**, former homeland security secretary; and William Lynn, former deputy defense secretary, in an op-ed for the Washington Post in 2015.

"[E]ncryption is foundational to the future...So spending time arguing about 'hey, encryption is bad and we ought to do away with it'...that's a waste of time to me."

-**Admiral Mike Rogers**, then director of the National Security Agency and Commander of U.S. Cyber Command, at an event in 2016 hosted by the Atlantic Council.

"I think I come down on the side of industry. The downsides of a front or back door outweigh the very real public safety concerns... a hole is a hole... Given that reality, Americans are well-served by a high water level of security for everyone."

-**General Michael Hayden**, former director of the National Security Agency and the Central Intelligence Agency, at the Aspen National Security Forum in 2015.

"[T]he US Government should: [1] fully support and not undermine efforts to create encryption standards; [2] not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and [3] increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."

-**Final report** of the President's Review Group on Intelligence and Communications Technologies in 2013, which included two former national security officials: Mike Morrell, former director of the Central Intelligence Agency; and Richard Clarke, former White House anti-terror czar.

"[F]or the Department of Defense[,] data security including encryption is absolutely essential to us. None of our stuff works unless it's connected... So we're foursquare behind strong data security, including strong encryption... I'm not a believer in back doors or a single technical approach to what is a complex and complicated problem. I'm just not. I don't think that's realistic. I don't think that's technically accurate."

-**Dr. Ash Carter**, then Secretary of Defense, at the 2016 RSA conference.

United Kingdom:

"Encryption is an overwhelmingly good thing—it keeps us all safe and secure... Building in back doors is a threat to everybody and it's not a good idea to weaken security for everybody to tackle a minority."

-**Robert Hannigan**, the former Director of the United Kingdom's Government Communications Headquarters (GCHQ), responding to questions about Home Secretary Amber Rudd's 2017 plan to mandate encryption backdoors in the Independent.

"The solution is not, of course, that encryption should be weakened, let alone banned. But neither is it true that nothing can be done without weakening encryption. I am not in favour of banning encryption just to avoid doubt. Nor am I asking for mandatory backdoors."

-**Robert Hannigan**, then Director of the United Kingdom's Government Communications Headquarters (GCHQ), at the Massachusetts Institute of Technology in 2016.

"We have a dialogue with many of these companies about how they can help more, that doesn't mean you need to have a backdoor, a secret key or something like that, that is not something that I think is realistic to be asking from these companies."

-**U.K. Home Secretary Sajid Javid** speaking to Politico in 2018.

The Netherlands:

"There are currently no options in a general sense, e.g. via standards, to weaken encryption products without compromising the security of digital systems that use encryption...The cabinet is therefore of the opinion that at this point in time it is not desirable to take restrictive legal measures as regards the development, availability and use of encryption in the Netherlands."

-**G.A. Van der Steur**, then Minister of Security and Justice, and H.G.J. Kamp, then Minister of Economic Affairs, Dutch Executive Cabinet 2016 Statement on Encryption

Germany:

"The use of encryption and other security mechanisms is necessary to ensuring Internet safety...We support the use of more and better encryption and aim to be the world's leading country in this area. To achieve this goal, the encryption of private communication must be adopted as standard across the board."

-**Federal Government** Digital Agenda 2014-2017

"Secure encrypted e-mail communication remains an important and appropriate means of increasing information security... We are firmly committed to making Germany the number one encryption location."

-**Arne Schönbohm**, President of BSI of the Bundesamt für Sicherheit in der Informationstechnik, Germany's Federal Office of Information Security, in a 2018 press release.

France:

"Robust encryption solutions, completely under the user's control, contribute to the balance and the security of the digital ecosystem. The introduction of backdoors or master keys would lead to a weakening of the security of technical solutions deployed currently, which would be damaging to the information assets of companies, the stability of the digital economy's ecosystem and the protection of individual freedoms."

-**Commission Nationale de l'informatique et des Libertés** [CNIL] 2017 statement.

"Personal data are no longer protected [with an encryption backdoor]...Even if the intention [to give the police the means] is commendable, it also opens the door to actors who have less laudable intentions, not to mention the possible economic damage to undermine the credibility of the companies that foresee these flaws."

-**Then Deputy Axelle Lemaire**, digital affairs minister of the Socialist Party [Parti Socialiste] statements on the 2016 Kosciusko-Morizet encryption backdoor proposal.

"Among the most important protection tools are cryptography and especially information encryption technologies. They alone make it possible to ensure security [of] sensitive digital data. And to quote, pell-mell, exchanges covered by the secrecy of national defense, health data, [...] the strategic data of companies, the personal data of citizens."

-**Guillaume Poupard**, Director General of France's national cybersecurity agency, l'Agence nationale de la sécurité des systèmes d'information [Anssi], commenting on a 2016 proposal to mandate encryption backdoors.

For more information, visit newamerica.org/oti