What The Experts Say About Encryption

I am deeply worried about the magical thinking that I think is taking place among some in law enforcement that back doors can be created, that devices can be hacked into in a good way but not in a bad way.
Julie Brill, former Commissioner, Federal Trade Commission
The Wrap's Power Women Breakfast, March 2016

[*E]ncryption is a necessary part of data security, and strong encryption is a good thing.*
Ash Carter, Secretary, Department of Defense
"Securing the Oceans, the Internet, and Space: Protecting the Domains that Drive Prosperity," March 2016

[W]e still need encryption and with the challenges we face on cybersecurity, encryption remains even more essential to protecting safety and commerce online.
Alan Davidson, Director for Digital Economy, U.S. Department of Commerce
Access' Crypto Summit, July 2015

As a person charged with thinking about consumer protection, I deeply worry about things like mandatory backdoors and exceptional-access systems in consumer-facing products ... It has the consequence of potentially making consumer data less secure.
Terrell McSweeny, Commissioner, Federal Trade Commission
State of the Net conference, January 2016

Now, more than ever, strong security and end-user controls are critical to protect personal information ... If consumers cannot trust the security of their devices, we could end up stymieing innovation and introducing needless risk into our personal security. In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers.
Terrell McSweeny, Commissioner, Federal Trade Commission
"Worried About Your Data Security? How Encryption Can Help Protect Your Personal Information," September 2015

Specifically, companies should: (1) conduct a privacy or security risk assessment as part of the design process; (2) test security measures before products launch; (3) use smart defaults – such as requiring consumers to change default passwords in the set-up process; (4) consider encryption, particularly for the storage and transmission of sensitive information, such as health data; and (5) monitor products throughout their life cycle and, to the extent possible, patch known vulnerabilities.
Edith Ramirez, Chairwoman, Federal Trade Commission
"Privacy and the IoT: Navigating Policy Issues," International Consumer Electronics Show, January 2015

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org

Strong encryption makes us safe.
Jessica Rosenworcel, Commissioner, Federal Communications Commission
The Wrap's Power Women Breakfast, March 2016

Encryption is foundational to the future. So spending time arguing about 'encryption is bad and we ought do away with it'— that is a waste of time to me. Encryption is foundational to the future.
Admiral Michael S. Rogers, Commander of US Cyber Command and Director of the National Security Agency
US Cybercom and the NSA, Atlantic Council, January 2016

Much of GCHQ's work is on cyber security, and given the industrial-scale theft of intellectual property from our companies and universities, I'm acutely aware of the importance of promoting strong protections in general, and strong encryption in particular. The stakes are high and they are not all about counter terrorism.
Robert Hannigan, Director, GCHQ, UK
"Front doors and strong locks: encryption, privacy and intelligence gathering in the digital era," MIT, March 2007

Even if the intention [to empower the police] is laudable, it also opens the door to the players who have less laudable intentions, not to mention the potential for economic damage to the credibility of companies planning these flaws. You are right to fuel the debate, but this is not the right solution according to the Government's opinion.
Axelle Lemaire, Digital Affairs Minister, France
Remarks rejecting an encryption amendment to France's Digital law, January 2016

"The new rules should also clearly allow users to use end-to-end encryption (without 'backdoors') to protect their electronic communications… Decryption, reverse engineering or monitoring of communications protected by encryption should be prohibited. In addition, the use of end-to-end encryption should also be encouraged and when necessary, mandated, in accordance with the principle of data protection by design…"

Giovanni Buttarelli, European Data Protection Supervisor (EDPS)
Preliminary EDPS Opinion on the Review of the ePrivacy Directive (2002/58/EC)

20 F Street, NW, Suite 800
Washington, DC 20001
P 202-872-5500
W bsa.org