President Barack Obama
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

October 7, 2015

Dear Mr. President,

As organizations committed to free markets and limited government, we urge your administration to take a clear stand in support of the individual's right to protect his or her security and privacy with strong encryption technology — and against efforts to weaken encryption technology, both in the U.S. and around the world. Good cybersecurity begins at home — with encryption.

As a recently leaked policy memo from the National Security Council notes, "the benefits to privacy, civil liberties, and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption." The memo concludes that encryption is the "strongest option for cybersecurity, economic competitiveness and civil liberties and human rights." This is precisely the position the U.S. should take – both for the sake of its own citizens and to maintain its global leadership and moral authority on Internet Freedom.

Some U.S. law enforcement agencies claim their online investigatory and tracking capabilities may be "going dark": that strong encryption is frustrating their ability to investigate, apprehend, and prosecute criminals and terrorists. But officials have yet to substantiate such claims. According to the Department of Justice's own 2014 statistics, out of a total 3,554 state and federal wiretap orders, in only four cases did law enforcement encounter strong, unbreakable encryption.

Yes, encryption can indeed help terrorists and criminals to communicate in secret, just as almost *any* widely available technology, from automobiles to firearms, can also be used for unlawful purposes. But the mere *possibility* of nefarious agents abusing these tools does not automatically justify banning them. Encryption's economic benefits far outweigh its potential costs, as the National Security Council policy memo notes. Just as the Clinton Administration took a hands-off approach to the growth and development of the commercial Internet, so too should your Administration ensure the continued growth of the Internet by promoting the use of encryption as the basis for both cybersecurity and privacy.

America's global leadership rests on two pillars: its economic strength and its moral authority. Defending encryption would promote both, enabling Internet services to flourish, making users more safe and secure online, and allowing them to communicate and associate in private. Restricting encryption would:

- Drive Internet entrepreneurs overseas and make it harder for existing American businesses to compete
- Validate the widespread perception that the U.S. government has unrestricted access to private data that flows through American servers
- Help those countries that are trying to reduce cross-border data flows and require data about their citizens to be hosted in their own countries; and
- Play into the hands of governments that want to monitor Internet use to suppress dissent.

We urge your Administration to consider the full ramifications of weakening or limiting encryption. There is no such thing as a backdoor that *only* the US government can access: any attempt to weaken encryption means making users more vulnerable to malicious hackers, identity thieves, and repressive governments. America must stand for the right to encryption — it is nothing less than the Second Amendment for the Internet.

Thank you,

Niskanen Center
TechFreedom
FreedomWorks
R Street Institute
Students For Liberty
Citizen Outreach
Downsize DC
Institute for Policy Innovation
Less Government
Center for Financial Privacy and Human Rights
American Commitment