Computer & Communications
Industry Association
Tech Advocacy Since 1972

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

October 7, 2015

Dear Mr. President,

I have great respect and empathy for those in our intelligence and law enforcement communities who work to keep our nation safe and secure by utilizing all the surveillance and technical tools available to them. Their mission is a challenging one, and it is understandable that they should seek to expand their technical capabilities whenever possible.

However, regardless of good intentions, any efforts to undermine the security and effectiveness of strong encryption are misguided, shortsighted, impractical, and ultimately counterproductive.

I understand there is ongoing discussion within your Administration regarding the growing availability of strong encryption in consumer products and communications systems, and the implications this might have for criminal and counterterrorism investigations. Technical and legislative policy proposals, from mandates to incentives, are being debated by a variety of stakeholders. It is tempting to believe that some compromise that would fully satisfy all interested parties—from law enforcement to consumer advocates—is feasible.

That simply is not the case. Computer security experts, including those in your Administration, have come to one conclusion about attempts to build third-party or government access into already-complex encryption systems. Such backdoors rarely remain secure and instead become means for unlawful access by criminals or others inclined to misuse such access.

These risks are not just theory. Backdoors intended merely for permissible uses have regularly been breached to the public's detriment in the past. Weakening or curbing the use of encryption would simply serve to exacerbate the significant existing problems of data breaches and identity theft plaguing consumers, which have substantial adverse economic effects for individuals and companies alike.

The tech community is perhaps uniquely appreciative of the importance of user privacy and security in preserving the open and free environment in which ideas can be freely communicated, innovations inspired, and individuals empowered. Confidence in the integrity and security of the Internet and associated technologies is essential for its continued success as a platform for digital speech and commerce. Any domestic attempts to weaken strong encryption tools would have significant international consequences for online expression and economic growth.

The approach your Administration takes on citizens' adoption of secure communications technologies and encryption would certainly receive international scrutiny and could tragically be used to lower the bar on privacy and civil liberties protections abroad. Individuals both here and abroad need to be able to shield themselves from the prying eyes of hackers, identity thieves, stalkers—and indeed, their governments.

Computer & Communications
Industry Association
Tech Advocacy Since 1972

The inability to communicate securely would have a chilling effect on the the speech of dissidents and journalists worldwide.

Already, earlier statements made by Administration officials have been mirrored by legal requirements for backdoors in tech products and source code disclosure in China, along with interference with encrypted VPN services used by activists and the press. Similar proposals to weaken encryption standards have recently been made in India. Sadly, any effort to prevent individual and institutional self-protection by democratic law enforcement and political leaders will be cheered and emulated by authoritarian regimes fearful of citizen empowerment in their countries. As a past chairman and member of the State Department's Advisory Committee on International Communications & Information Policy, I am aware that issues of information freedom and free speech are never just domestic or international.

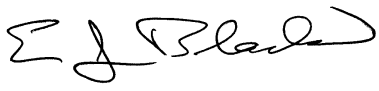
The global competitiveness of the U.S. tech industry has already been damaged by the last two years of disclosures of mass surveillance by U.S. intelligence agencies. Further eroding the trust of users worldwide by requiring government access to secure products or systems, or seeking voluntary modifications in their design, would simply lead to more customers lost to international competitors. I am hopeful that your Administration will choose a path that supports the global competitiveness of our leading industries and helps protect the privacy and security rights of individuals.

In view of the far-reaching impacts of your Administration's position on the availability and rigor of secure communications technologies, it is heartening to hear that a range of interested agencies are involved in the deliberative process. Given the substantial economic benefits that stem from the widespread availability of strong encryption, not to mention its essential role in free expression online, I urge your Administration not just to forgo limitations on its use, but to support and promote its adoption worldwide.

History will likely judge that one of the most important developments of our era was the development and evolution of the Internet. Whether it becomes an enduring positive empowering force for human freedom or a tool for surveillance, censorship, and control of the individual is yet to be determined.

Thank you for your attention.

Sincerely,



Ed Black
President & CEO
Computer & Communications Industry Association

900 17th Street NW Suite 1100 Washington, DC 20006 P: (202) 783-0070 F: (202) 783-0534 www.ccianet.org