
July 7, 2015

The Honorable Barack Obama
President
1600 Pennsylvania Ave. NW
Washington, DC 20500

Dear Mr. President,

I write to request that you reconsider efforts within your administration to force U.S. companies to reduce the security they provide customers. We believe any effort to forcibly weaken data encryption will harm U.S. citizens and increase the likelihood of catastrophic breaches.

ACT | The App Association represents over 5,000 app makers and technology companies creating mobile applications in the world's most important fields, including healthcare, enterprise, and education. The organization is widely recognized as the foremost authority on the intersection of government and the app economy.

Our members' success is founded on earning the trust of their customers. As hospitals, banks, and factories adopt mobile functionality, security becomes a key decision point when moving data to the cloud. Unfortunately, recent statements by the Department of Justice (DoJ) denigrating encryption threaten to destroy that trust and weaken our ability to protect consumers. Surprisingly, these statements come at the very moment when the Office of Personnel Management's (OPM) failure to properly encrypt sensitive data has led to a massive, potentially devastating, breach of federal worker's personal information.

On October 16, 2014, FBI Director James Comey addressed a Brookings Institution briefing on encryption to discuss what the FBI calls "going dark"—a term describing law enforcement's inability to easily access Americans' private encrypted communications. The briefing was an opportunity for the Director to defend himself against critics assailing the bureau for proposals that would do more to help criminals than secure data.

Instead, Director Comey went the other direction: "[w]e aren't seeking a back door approach. We want to use the front door, with clarity and transparency, with clear guidance provided by law." Alarm spread within the cryptography, security, and privacy communities with the realization that our country's top law enforcement officer fundamentally misunderstood the principles of electronic encryption. The manner in which he was asking the Administration and Congress to modify encryption law would result in disastrous, unforeseen consequences.

Requiring law enforcement access to encrypted communications would multiply potential points of failure in software security systems, increasing their susceptibility to data breach and theft. It is simply impossible for app makers and software companies to bootstrap additional access features onto existing encryption architectures. Moreover, creating an effective encryption product that provides law enforcement back door entry is beyond the reach of our understanding of mathematical cryptography.

Encryption methods are based on highly complex principles of mathematical cryptography. The common encryption scheme, RSA, for example, manipulates prime numbers over 600 decimals long to achieve satisfactory encryption. Any lawful access feature applied to an encryption system would require

cryptographers to add additional mathematical manipulations to existing cryptographic processes. Encryption architects do not understand how to provide built-in access for law enforcement even at an abstract, theoretical level.

Beyond the theoretical, we have real world experience in the failure that results from requiring law enforcement access to encryption products. In the 1990s, the National Security Agency attempted to introduce hardware that simultaneously provided strong encryption and law enforcement access. It was called the Clipper Chip. Within a year of the chip's debut, security researchers had already revealed serious technical vulnerabilities that rendered it useless. Efforts to re-deploy the Clipper Chip never materialized, and the program died on the vine.


The simple fact, exemplified by the experience of the Clipper Chip, is that any additional point of entry engineered into an encryption scheme—whether a “back door,” a “front door,” a “golden key,” or a “lawful access point”—is simply an open door through which any criminal may walk. We can either have strong security *or* we can have law enforcement access encrypted communications, but we cannot have both.

The United States is home to the world's most vibrant app economy—one that is predicted to grow to over \$150 billion annually by 2017. Providing data security is a crucial product differentiator for U.S. app companies competing in the global economy. As the Office of Personnel Management breach recently demonstrated, security can only be guaranteed through strong encryption. Forcing U.S. app companies to weaken their encryption through inclusion of a back door not only threatens the privacy and security of those companies' clients' data, but also puts those companies at a significant competitive disadvantage to their foreign counterparts.

ACT | The App Association and our member companies respect the important role our nation's law enforcement plays in protecting our citizens. We feel the same responsibility in the conduct of our business practices and the protection of our customers' data. For these reasons, we strongly urge you to oppose any government efforts to weaken encryption standards.

We welcome the opportunity to work with your administration to ensure the safety of American citizens in a manner that does not undermine their data security.

Respectfully,

A handwritten signature in black ink that reads "Jonathan Zuck". The signature is written in a cursive, slightly slanted style.

Jonathan Zuck
President