ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

Obama's Silence on Crypto Could Set the Stage For Bad Policies to Come

Rainey Reitman

October 27, 2016

One year ago today, the 100,000th person added their name to a public petition calling on President Obama to categorically reject any attempt to add backdoors to our devices or otherwise undermine encryption.

Since then, crickets.

Obama has promised to reply to petitions on his *We the People* platform that receive over 100,000 signatures. But the only response our hugely popular petition received was a nonresponse asking for more input.

Since then, the issue has become even more pressing. While the urgency of the Apple encryption battle may have abated, the conversation around forcing tech companies to assist the government in obtaining access to unencrypted data has continued.

Julian Sanchez, a senior fellow at the Cato Institute, wrote last month that the misguided Feinstein-Burr proposal—which sought to force tech companies to render unencrypted communications at law enforcement's request—has been revised by the authors with an intent to find a version they could push through Congress with less opposition. Sanchez wrote: "Their offices have been circulating a series of proposed changes to the law, presumably in hopes of making it more palatable to stakeholders," and then he detailed the adjustments to the fundamentally flawed proposal.

This should worry anybody who believes in strong digital security and fears attempts to undermine it.

The backdoor issue is part of a larger conversation our country is having about digital security right now. We saw renewed public interest in cybersecurity last week when major websites like Twitter, Amazon, and Paypal suffered outages as their DNS provider Dyn came under a series of DDoS attacks. This highlights how the choices independent corporations make around security can have huge ramifications for the general public. We now know that the attacks last week were at least partially reliant on the security choices made by companies like Hangzhou Xiongmai, whose default settings made it trivial for their products to be taken over and turned into a zombie hoard that helped take down some of the Web's favorite sites. In light of this demonstration of how poor security can cripple core Internet services, it's even more important that the U.S. government champion best practices. We need the Administration to be leading our

country along the path of strong security practices, uncompromised crypto, and engineering design that's resistant to attack.

EFF, Access Now, and others sent a letter to the president today, urging him again to respond to the 100,000 individuals who spoke out in defense of encryption. As we explain in our letter, the world is watching the United States to see how we'll address this issue:

Around the world, governments have capitalized on the lack of leadership in support for encryption and implemented harmful laws and policies. China specifically cited to the rhetoric in the U.S. last December when it passed a new law that likely bans end to end encryption, with no upper limit on fines for non-compliant companies. The UK is on the fringe of passing a law that would, practically, have the same impact. And from Brazil to Russia to India we are seeing other actions that will undermine the security of the global Internet.

Obama has tried to paint himself as a tech-savvy president who champions civil liberties. As he prepares to leave office in a few months, he has a golden opportunity to stand up for digital security. That means doing more than quietly indicating he wouldn't support a backdoor bill; it means affirmatively describing a policy of the federal government that doesn't seek to undermine encryption.

Over 100,000 people have been waiting for Obama's leadership on this vital issue for a year now. His continued silence on the matter could leave open questions about how and when the Justice Department will seek future methods of undermining our security. But a strong statement from the White House today could ensure his Justice Department stops its nonsensical and short-sighted war on secure communications. It will also set the right standard for the next president to take office.

We're all counting on you, Mr. President.