Trump Administration Is Coming After Encrypted Privacy Applications

by Trevor Timm via stacey - Medium *Friday, Aug 2 2019, 9:02pm*
international / prose / post

> *The attempt by government to gain access to our last right to privacy and ESSENTIAL security is brazen to the extreme. Put simply government and agencies want 'backdoors' to allow them easy access to encrypted software applications and hardware such as iPhones. Indeed, but forcing the creation of backdoors is self-defeating as it punches such a large hole in security that hacker kiddies could easily gain access and chaos would ensue as all our security, banking etc, could easily be hacked and no assurances are given by government for creating a picnic for hackers, such as compensation for such financial losses, as it is they/gov that forced the initial compromise. Not that government has ever given a damn about the people, it simply wants in, and we take all the risks as usual. Governments like this no nation needs.*

Attorney General William Barr has made clear his desire to dismantle the security of our encryption services.

Just as Americans face yet another devastating data breach — this time with the Capital One credit card servers — the Trump administration seems bent on weakening our collective cybersecurity even further.

It's hard to count the number of recent devastating cybersecurity episodes, whether it's on Capital One, Equifax, or the U.S. government itself. With these attacks on an uptick, it's been encouraging to see a corresponding rise in chat applications that offer end-to-end encryption — a boon to everyone's privacy and security.

Messaging apps like WhatsApp, iMessage, and Signal provide consumers strong safeguards, where everyone's messages are encrypted by default — even the companies that own the message applications can't access them. These services are collectively providing billions of people with protections to prevent their messages from landing in the next massive data dump (not to mention helping to protect everyone from government mass surveillance). Device encryption, too, is becoming standard on cellphones. Even Apple, for example, can't unlock an iPhone that is encrypted with a passcode.

But Attorney General William Barr wants to change all that. Last week, he delivered an ominous speech in which he claimed the U.S. government's patience with tech companies offering strong encryption is wearing thin, and that a law banning strong encryption or requiring companies build in back doors for the government could soon become a reality.

Even though Barr said improving cybersecurity was a "national imperative" — he added that the government would "welcome these improvements to privacy and security, and will work to preserve and strengthen them" — he then spent the entirety of his talk explaining the government's desire to weaken these same technologies that are protecting billions of people so that it might gain access to conversations when it pleases.

"By enabling dangerous criminals to cloak their communications and activities behind an essentially

impenetrable digital shield, the deployment of warrant-proof encryption is already imposing huge costs on society," Barr claimed. "It seriously degrades the ability of law enforcement to detect and prevent crime before it occurs."

While Barr acknowledges it's clear that end-to-end encryption (which he dubbed "irresponsible encryption") provides some consumer protections, he claims it weakens people's overall safety and national security at the same time.

Barr acts is if consumer protection is small bore compared to national security. First, encryption is protecting more than just our private information. After Apple implemented strong encryption protections on the iPhone, phone theft — one of the most common crimes in New York City — plummeted because the phones became almost useless to criminals. Of course, phone thefts, when done by robbery, can often become violent.

Protecting this type of information is also a national security issue. After the Clinton campaign was hacked in 2016, Clinton staffers were told to move over to Signal to better protect their communications from foreign governments.

Since then, use of encrypted apps by aides in Congress and campaign staff has only increased. In fact, there's an easy story any journalist can write if the debate over encryption heats up again in Congress. To any lawmaker who is advocating for a ban on strong encryption, simply ask them: Do you, your staff, or your campaign use Signal or another encrypted messaging app to protect your communications? The answer will most likely be yes.

Of course, this is not to say that criminals will never use encrypted messaging apps. It's true that surveilling the content of messages may be a little harder for governments, but they are also operating in what many have called "the golden age of surveillance," where virtually everyone carries around a cellphone 24/7, which can act as a tracking beacon for their exact whereabouts, who they are talking to, and how often.

Security experts across the political spectrum (even some well-known former intelligence officials) have explained that creating a back door opens up all sorts of cybersecurity nightmares, and we are in a much better position providing more protections for our data, not less. If the companies can access our data, and the FBI can as well, it's inevitable that foreign governments or criminals will too.

It's also hard to trust anything Barr says on the subject. The U.S. government has a long history of exaggerating and even making up claims about the supposed dangers of encryption. Under the Obama administration, former FBI Director Jim Comey pushed hard for a new law that would ban end-to-end encryption, and the Justice Department even attempted to force Apple to unlock iPhones via a court order. Only later did they admit, once they lost the fight, that they were misleading the public and Apple's phone weren't nearly as "unbreakable" as they made it seem.

Banning strong encryption is a terrible idea no matter the administration in charge. But why should anyone trust Donald Trump, of all people, with this incredible new power?

https://gen.medium.com/the-trump-administration-is-coming-after-whatsapp-be6715ceec73

Inverse Times Open Publishing. http://inversetimes.lingama.net/news/story-760.html