The Washington Post
29 July 2015

Why the fear over ubiquitous data encryption is overblown

Clarification: Due to a production error, a version of this column was temporarily posted prematurely before the editing process was complete.

Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies.

The Washington Post
28 July 2015

Why the fear over ubiquitous data encryption is overblown

Mike McConnell was director of the National Security Agency under President Clinton and director of national intelligence under President George W. Bush. Michael Chertoff was homeland security secretary under Bush. William Lynn was deputy defense secretary under President Obama.

The Washington Post

NOT NOW ?

Get the Today's Headlines Newsletter

Free daily updates delivered just for you.

National

Editor’s note

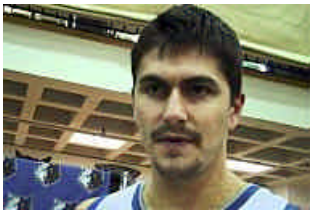
December 31, 2010

This file was inadvertently published.

PROMOTED STORIES

Recommended by

10 Reasons A Dog Will Attack Its Owner
Poundwishes



The 20 Worst NBA Draft Picks Ever
Worthly

The 20 Easiest Dogs for First-Time Owners
PetBreeds

Hydrogen Is The Most Abundant Element In The
Toyota

Take a Trip to Connecticut’s Beautiful Coast This
CT Tourism

Paula Creamer's Husband Flies Her To The Women's
espnW

You have reached the cached page for **https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html**

Below is a snapshot of the Web page as it appeared on **7/28/2015** (the last time our crawler visited it). This is the version of the page that was used for ranking your search results. The page may have changed since we last cached it. To see what might have changed (without the highlights), go to the current page.

The Washington Post

Opinions

Why the fear over ubiquitous data encryption is overblown

By Mike McConnell, Michael Chertoff and William Lynn July 28 at 8:01 PM

Mike McConnell was director of the National Security Agency under President Clinton and director of national intelligence under President George W. Bush. Michael Chertoff was homeland security secretary under Bush. William Lynn was deputy defense secretary under President Obama.

More than three years ago, as former national security officials, we penned an op-ed to raise awareness among the public, the business community and Congress of the serious threat to the nation's well-being posed by the massive theft of intellectual property, technology and business information by the Chinese government through cyberexploitation. Today, we write again to raise the level of thinking and debate about ubiquitous encryption to protect information from exploitation.

In the wake of global controversy over government surveillance, a number of U.S. technology companies have developed and are offering their users what we call ubiquitous encryption — that is, end-to-end encryption of data with only the sender and intended recipient possessing decryption keys. With this technology, the plain text of messages is inaccessible to the companies offering the products or services as well as to the government, even with lawfully authorized access for public safety or law enforcement purposes.

The FBI director and the Justice Department have raised serious and legitimate concerns that ubiquitous encryption without a second decryption key in the hands of a third party would allow criminals to keep their communications secret, even when law enforcement officials have court-approved authorization to access those communications. There also are concerns about such encryption providing secure communications to national security intelligence targets such as terrorist

organizations and nations operating counter to U.S. national security interests.

Several other nations are pursuing access to encrypted communications. In Britain, Parliament is considering requiring technology companies to build decryption capabilities for authorized government access into products and services offered in that country. The Chinese have proposed similar approaches to ensure that the government can monitor the content and activities of their citizens. Pakistan has recently blocked BlackBerry services, which provide ubiquitous encryption by default.

We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

First, such an encryption system would protect individual privacy and business information from exploitation at a much higher level than exists today. As a recent MIT paper explains, requiring duplicate keys introduces vulnerabilities in encryption that raise the risk of compromise and theft by bad actors. If third-party key holders have less than perfect security, they may be hacked and the duplicate key exposed. This is no theoretical possibility, as evidenced by major cyberintrusions into supposedly secure government databases and the successful compromise of security tokens held by the security firm RSA. Furthermore, requiring a duplicate key rules out security techniques, such as one-time-only private keys.

Second, a requirement that U.S. technology providers create a duplicate key will not prevent malicious actors from finding other technology providers who will furnish ubiquitous encryption. The smart bad guys will find ways and technologies to avoid access, and we can be sure that the "dark Web" marketplace will offer myriad such capabilities. This could lead to a perverse outcome in which law-abiding organizations and individuals lack protected communications but malicious actors have them.

Finally, and most significantly, if the United States can demand that companies make available a duplicate key, other nations such as China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications

to a wide spectrum of governmental access regimes with varying degrees of due process.

Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interests. After all, political power and military power are derived from economic strength. If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential. And that imperative may outweigh the tactical benefit of making encrypted communications more easily accessible to Western authorities.

History teaches that the fear that ubiquitous encryption will cause our security to go dark is overblown. There was a great debate about encryption in the early ’90s. When the mathematics of “public key” encryption were discovered as a way to provide encryption protection broadly and cheaply to all users, some national security officials were convinced that if the technology were not restricted, law enforcement and intelligence organizations would go dark or deaf.

As a result, the idea of “escrowed key,” known as Clipper Chip, was introduced. The concept was that unbreakable encryption would be provided to individuals and businesses, but the keys could be obtained from escrow by the government under court authorization for legitimate law enforcement or intelligence purposes.

The administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the ’90s and into the new century.

Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.

Read more on this issue:

The Post’s View: Putting the digital keys to unlock data out of authorities’ reach

The Post’s View: Compromise needed on smartphone encryption

Cyrus R. Vance Jr.: Apple, Google threaten public safety with default smartphone encryption