

From the Very Creation of the Internet, U.S. Spy Agencies Fought to Block Encryption

By [Washington's Blog](#)

Global Research, May 26, 2015

[Washington's Blog](#) 24 May 2015

Region: [USA](#)

Theme: [Intelligence](#), [Police State & Civil Rights](#)

American spy agencies have intentionally weakened digital security [for many decades](#). This [breaks the functionality of our computers and of the Internet](#). It reduces functionality and reduces security by – for example – [creating backdoors that malicious hackers can get through](#).

The spy agencies have treated patriotic Americans who want to use encryption to protect their privacy as [extremists ... or even terrorists](#).

As Gizmodo's Matt Novak [points out](#), this attack started at the very birth of the internet:

In the 1970s, civilian researchers at places like IBM, Stanford and MIT were developing encryption to ensure that digital data sent between businesses, academics and private citizens couldn't be intercepted and understood by a third party. This concerned folks in the U.S. intelligence community who didn't want to get locked out of potentially eavesdropping on anyone, regardless of their preferred communications method. Despite their most valiant efforts, agencies like the NSA ultimately lost out to commercial interests. But it wasn't for lack of trying.

When the NSA got wind of the research developments at IBM, Stanford and MIT in the 1970s they scrambled to block publication of their early studies. When that didn't work, the NSA sought to work with the civilian research community to develop the encryption. As Stowsky writes, "the agency struck a deal with IBM to develop a data encryption standard (DES) for commercial applications in return for full pre-publication review and right to regulate the length, and therefore the strength of the crypto algorithm."

Naturally, in the Watergate era, many researchers assumed that if the U.S. government was helping to develop the locks that they would surely give themselves the keys, effectively negating the purpose of the encryption. Unlike IBM, the researchers at Stanford and MIT didn't go along with the standard and developed their own encryption algorithms. Their findings were published (again, against the wishes of the NSA) in the late 1970s after courts found that researchers have the right to publish on the topic of cryptography even if it makes the government uncomfortable. According to Stowsky, the NSA retaliated by trying to block further research funding that Stanford and MIT were receiving through the National Science Foundation.

Novak also notes that – right [from the start](#) – people realized the potential of the internet as a tool for conducting mass surveillance on the public. And see [this](#), [this](#) and [this](#).

The original source of this article is [Washington's Blog](#)
Copyright © [Washington's Blog](#), [Washington's Blog](#), 2015

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Washington's Blog](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca