ELECTRONIC FRONTIER FOUNDATION
PROTECTING RIGHTS AND DEFENDING FREEDOM ON THE ELECTRONIC FRONTIER eff.org

The Crypto Wars

GOVERNMENTS WORKING TO UNDERMINE ENCRYPTION

Revelations from whistleblower Edward Snowden exposed the NSA's long-standing, systematic effort to weaken and sabotage commercially available encryption used by individuals and businesses around the world.

This means that even when we believe that we are communicating using trustworthy and secure methods, our information and activities may be compromised by security vulnerabilities inserted into systems by governments—often known as "backdoors" because they provide the government with access, but also leave an opening for malicious actors.

This practice puts our data (financial records, business secrets, email, web browsing, medical and legal records) and devices (smartphones, computers, and even connected devices like smart watches or webcams)—all computing that relies on a level of security—at risk. Yet intelligence officials, especially the director of the FBI, are loudly advocating for unfettered access to encrypted data.

Fighting for or against cryptography is a battle known as the "Crypto Wars".

We thought this battle was over. In the 1990s, EFF led the fight to protect users' ability to have strong, uncompromised encryption. In collaboration with leading academics, industry trade associations, and politicians from all over the world, we defeated U.S. President Clinton's "Clipper Chip" – a proposal to compel companies to give the government backdoor keys into commercial encryption technologies. We also defeated export regulations that effectively prevented the development and distribution of strong encryption. Law enforcement did succeed in one area—the Communications Assistance for Law Enforcement Act (CALEA) forced telephone companies to redesign their network architectures to make it easier for law enforcement to wiretap digital telephone calls. That, at least, wasn't done secretly.

The NSA undermined us all.

According to documents leaked to the New York Times, a project known as "BULLRUN" (note: NSA assigns their products multiple names) is the NSA's effort to bypass our democratic mechanisms and sabotage our security anyway—in secret. Many details of BULLRUN are still undisclosed, but we do know enough to be angry.

Say no to backdoors: eff.org/secret-surveillance-law

Now intelligence officials are ignoring computer security experts that say real security can't coexist with unfettered law enforcement access.

FBI Director James Comey and his colleagues in the intelligence community have been pushing the FBI's twenty-year-old talking points (**eff.org/deeplinks/2014/10/90s-and-now-fbi-and-its-inability-cope-encryption**) about why law enforcement must have special access to encrypted data—even though security experts have made it clear that's not possible. He and his supporters claim that information sources for law enforcement are “going dark”—but we're really in a golden age of surveillance.

An all-star group of computer security experts even published a statement explaining in detail why backdoor access is not feasible without sacrificing security. Yet Director Comey and his supporters continue to try to convince Congress and the public that there must be a technological solution.

We know that vulnerabilities are bad for everyone, and we'll fight against any attempts to weaken the cryptography and security that entire Internet relies on. But some damage has already been done.

What we know about how the government has weakened our infrastructure—all to make spying easier:

- The NSA has inserted hidden vulnerabilities into our security standards, resulting in NIST, the U.S. National Institute of Standards and Technology, withdrawing support from a key security standard that millions of products rely upon.
- The NSA made a $10 million deal with major security firm RSA to make Dual_EC_DRBG—an intentionally weakened random number generator—the default in its widely used BSAFE encryption toolkit.
- The FBI facilitates the NSA's efforts to weaken security with US companies.
- The NSA infiltrates companies to conduct this sabotage or works with companies to build weaknesses in systems, or coerces them into weakening their systems, all in secret.

Here’s what we all must do to protect our rights:

- Unlike proprietary software, open source software can be reviewed for vulnerabilities. Use and promote the use of open source encryption, like HTTPS Everywhere and Tor, to provide secure channels over insecure networks: **https://www.eff.org/https-everywhere**
- Check out EFF's Surveillance Self-Defense Guide for more tips on securing your data using better security practices and open-source tools: **https://ssd.eff.org**
- Join the developer community actively trying to make encryption stronger and more usable.
- Support organizations like the Electronic Frontier Foundation fighting to build and protect a secure and trustworthy Internet.

EFF is a member-supported non-profit. Join today at eff.org/join

Say no to backdoors: eff.org/secret-surveillance-law