Revelations from whistleblower Edward Snowden exposed the NSA’s long-standing, systematic effort to weaken and sabotage the encryption used by individuals and businesses around the world. Meanwhile, law enforcement officials from the director of the FBI to the Manhattan District Attorney to the UK’s Government Communications Headquarters (GCHQ) continue to seek special access to encrypted data.

Undermining encryption means that even when we believe we are using trustworthy and secure methods to communicate, our information and activities may be compromised by 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. Backdoors put 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) at risk.

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

We thought we won this battle. In the 1990s, EFF led the fight to protect users’ ability to have strong, uncompromised encryption. In collaboration with leading academics, industry associations, and politicians, we defeated the U.S. “Clipper Chip” 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, establishing the legal principle that “code is speech” protected by the First Amendment.

Then, we learned that the NSA undermined us all.

According to documents from the NSA, a project called “BULLRUN” was the NSA’s effort to bypass democratic mechanisms and sabotage the security of Internet users worldwide. Many details of BULLRUN are still undisclosed, but we do know that the U.S. government weakened our security infrastructure to make spying easier. In one publicly reported example, 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.
Now intelligence officials are ignoring computer security experts who say real security can't coexist with unfettered law enforcement access.

Intelligence and law enforcement officials, including former FBI Director James Comey, have revived twenty-year-old talking points about why law enforcement must have special access to encrypted data—even though computer security experts have made clear that's not possible to do safely. In 2015, an all-star group of experts even published an academic paper explaining in detail why backdoor access is not feasible without sacrificing security. Nevertheless, government officials still claim that sources of digital evidence are “going dark”—but we're really in a golden age of surveillance.

These arguments came to a head in early 2016, when the FBI tried to compel Apple to help unlock an iPhone used by one of the shooters in the 2015 San Bernardino attack. Because Apple had implemented full disk encryption and other security features in iOS, the FBI was unable to access the phone's contents as part of its investigation. Relying on the All Writs Act, a general-purpose law, the government argued that Apple was required to write and cryptographically sign custom code to defeat these security features, despite Apple’s strong practical and philosophical objections to backdooring its own code. EFF filed a brief in support of Apple, focusing on the significant First Amendment concerns involved in forcing a company to do this against its will. On the eve of a hearing, the FBI announced it had paid an outside contractor to take advantage of a security vulnerability in iOS to unlock the phone, meaning that no definitive legal outcome was reached.

Later that year, Senators Richard Burr and Dianne Feinstein drafted a bill that represented some of our worst fears in this new round of Crypto Wars. The Burr–Feinstein legislation would have forced Apple’s compliance with the All Writs Act order and imposed a sweeping duty on nearly all U.S. companies to decrypt any encrypted data they handled. In addition to its disastrous potential for computer security, the bill and similar proposals would be woefully ineffective, because encryption is globally available. EFF quickly organized opposition to the bill, and it failed to advance in the Senate.

Even though James Comey is no longer driving the FBI’s anti-encryption agenda, his successor, Director Christopher Wray has continued to try to convince Congress and the public that there must be a technological solution. Meanwhile, in late 2018, the GCHQ floated a proposal known as the “Ghost,” which would allow spy agencies to add a secret participant to end-to-end encrypted conversations. We know that vulnerabilities are bad for everyone, and we'll fight against any attempts to weaken the cryptography and security that the entire Internet relies on.

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.

The Electronic Frontier Foundation is the leading nonprofit defending digital privacy, free speech, and innovation. https://eff.org