The Crypto Wars

The ability to have a private conversation is a basic human right. In the online world, we need strong encryption to have true privacy and security. Without it, our democracies and our economies will break down. But governments around the world are working to sabotage the encryption used to keep us safe. Just in the last few years, the director of the FBI, the Manhattan District Attorney, the UK Parliament, and EU officials have all supported policies that put at risk our right to privacy.

When encryption is undermined, our data and activities can become known even when we believe we are using secure ways to communicate. These compromised systems have “backdoors,” which provide the government with special access—but also leave an opening for malicious actors. Backdoors put our data at risk: email, financial records, web browsing histories, medical and legal records, and business secrets. They also mean we can’t trust our own devices, like smartphones and even webcams.

The “Crypto Wars” Have Not Stopped

Since EFF’s founding, we’ve never stopped fighting for users’ right to strong, uncompromised encryption. In the 1990s, we worked with leading academics and industry associations, to defeat 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 prevented the development and distribution of strong encryption. And it was EFF lawyers who established the legal principle that “code is speech,” protected by the First Amendment. Today, encryption is more accessible, and protects more speech than ever before.

Despite these victories, intelligence and law enforcement officials continue to use twenty-year-old talking points about why they need special access to encrypted data—even though computer security experts have made clear that's not possible to do safely. There's no backdoor that works only for the good guys.

Lawmakers Keep Pushing to Break Encryption

Security experts have expressed overwhelming support for strong encryption. In 2021, a group of computer experts published "Bugs in Our Pockets," an academic paper explaining how backdoor access for governments—including client-side scanning—isn't compatible with our privacy and security. That follows other expert papers that drew the same conclusion. It is technologically impossible to give governments an encryption backdoor without weakening privacy and security for everyone.

But policymakers, misled by law enforcement and intelligence officials' false claims about "going dark," continue to push for ways to get around, or simply break, encryption. Since 2020, Senators Richard Blumenthal and Lindsey Graham have repeatedly introduced the "EARN IT Act," which would empower state legislators to undermine encryption in the name of fighting crime. The bill didn't pass, thanks to strong opposition from security experts and users.

These mass surveillance plans aren't limited to the U.S. In the European Union, a sweeping proposal would compel technology companies to scan and analyze their users' messages, including encrypted chats. Email, texts, social media messages, and DMs could all be subject to plain-text access and scanning.

In 2025, in response to the U.K.'s demands for a backdoor, Apple stopped offering users in the U.K. Advanced Data Protection, an optional feature in iCloud that turns on end-to-end encryption for files, backups, and more.

In country after country, when EFF supporters have spoken up about our rights to use encryption and speak freely—in court, and in the streets—we've won. We know that backdoors are bad for everyone, and we'll fight against any attempts to weaken the cryptography and security that the entire Internet relies on.

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