

Public Forum Debate Topic (NSDA, Nov-Dec 2025)

Resolved: *The U.S. should require technology companies to provide lawful access to encrypted communications.*

BACKGROUND

Encryption is a security technology that transforms information into a code that only the intended reader can understand using a special key. It works like a locked safe—only someone with the right key can open it and see what is inside. Today, encryption is used by millions of people every day to protect their emails, text messages, photos, banking information, and other private data.

There are two main types of encryption in common use. End-to-end encryption means that the technology company itself cannot read messages because it does not hold the decryption key—only the sender and receiver can read the messages. The other type allows companies to maintain access to the keys, which means they can read encrypted information if they possess the proper key.

Law enforcement officials, including the Federal Bureau of Investigation (FBI), argue that encryption makes it impossible for them to investigate serious crimes such as child exploitation, terrorism, human trafficking, and drug trafficking—even when they have a court order that gives them legal permission to access the information. This creates what they call a "lawless space" where criminals can operate without fear of detection.

However, computer scientists, privacy advocates, and technology companies raise serious concerns. They warn that if the government requires companies to provide access to encrypted communications, it would weaken encryption for everyone. This is because any "backdoor" or special access point created for law enforcement could potentially be discovered and exploited by hackers, foreign governments, or other bad actors. If encryption is weakened, criminals could use the same weakness to steal private information from ordinary people, including their bank account details, medical records, and personal secrets.

The debate asks a central question: Should we sacrifice the privacy and security of all citizens in order to give law enforcement better tools to investigate crimes? Or should we protect strong encryption for everyone, even if it makes some investigations more difficult? This is a question about balancing two important values: public safety and personal privacy.

PRO: REQUIRING LAWFUL ACCESS TO ENCRYPTED COMMUNICATIONS

1. Protecting Children from Exploitation: Law enforcement needs access to encrypted communications to identify and stop people who sexually abuse children. Predators use encrypted apps to hide their crimes and communicate with victims without fear of being caught. When police have a court order and cannot access encrypted messages, they cannot rescue children who are exploited or bring the criminals to justice.

2. Stopping Terrorism Before It Happens: Terrorists plan attacks using encrypted messaging apps. Law enforcement agencies argue that they need to access these communications to detect threats before attacks occur. Without lawful access, dangerous individuals can coordinate attacks while hiding from police detection, putting thousands of innocent lives at risk.

3. Investigating Serious Crimes: Murder, kidnapping, drug trafficking, and human trafficking—law enforcement says that encrypted devices and communications often contain crucial evidence for these serious crimes. When investigators cannot access this evidence, even with a valid search warrant from a judge, it becomes impossible to solve cases, catch criminals, and protect victims.

4. Balancing Privacy with Public Safety: Supporters of lawful access argue that this is not about mass surveillance. They say that law enforcement already has strong legal protections in place. Police must obtain a search warrant based on probable cause before accessing anyone's information. Just as police can enter homes with a warrant and open safes inside, they should be able to access encrypted data with the same legal protection.

5. Technology Companies Assisting in Other Ways: Technology companies already assist law enforcement in many ways. They provide subscriber information, location data, and metadata (information about communications rather than the content itself) in response to court orders. Companies have shown they can comply with legal requests while still protecting privacy. Requiring them to maintain the ability to decrypt data is consistent with existing legal requirements.

Public Forum Debate Topic (NSDA, Nov-Dec 2025)

Resolved: *The U.S. should require technology companies to provide lawful access to encrypted communications.*

PRO: REQUIRING LAWFUL ACCESS TO ENCRYPTED COMMUNICATIONS (Continued...)

6. Other Countries Are Adopting Similar Policies: The United Kingdom, Australia, and other democracies are implementing lawful access frameworks. If the United States does not adopt similar policies, American technology companies may face competitive disadvantages internationally. Additionally, if criminals know that only some countries require lawful access, they will simply move their criminal operations to countries with strict encryption protection.

7. Preventing the "Going Dark" Problem: As encryption becomes stronger and more widespread, law enforcement encounters an increasing number of cases where evidence is inaccessible despite legal authorization. In 2023, law enforcement conducted 2,101 wiretaps but could not decrypt the content in approximately ninety percent of the cases where they encountered encryption. This growing gap between legal authority and technical ability is a serious problem for public safety.

8. Protecting National Security: Intelligence agencies and military forces need to understand communications from foreign adversaries, terrorist organizations, and hostile nations. Without lawful access, the United States faces serious national security risks. Powerful nations like China and Russia actively work to decode American communications, yet the U.S. government cannot even access communications within its own borders due to encryption.

9. Victims Deserve Justice: Victims of crime and their families need law enforcement to be able to access evidence that might prove their case. When a phone is locked with encryption and contains evidence that could convict a murderer, rapist, or human trafficker, victims' voices may never be heard. These victims have a right to see criminals brought to justice, and law enforcement needs tools to make that possible.

10. Responsible Encryption is Possible: Supporters of lawful access argue that technology companies are intelligent enough to design encryption systems that protect user privacy while allowing law enforcement access with proper authorization. They point out that companies already maintain encryption keys for many services. It is possible to create systems where companies maintain the ability to decrypt data but only provide that access when served with a valid court order, just as banks must comply with search warrants.

CON: REJECTING LAWFUL ACCESS TO ENCRYPTED COMMUNICATIONS

1. Backdoors Cannot Be Kept Secret: Computer scientists agree that any backdoor or special access point created for law enforcement will eventually be discovered and exploited. Cryptography experts say that if you build a door that only "good guys" can use, bad guys will find it too. Once a backdoor exists, hackers, criminals, and hostile foreign governments can exploit it to access everyone's private information. There is no such thing as a "secret backdoor"—mathematics does not discriminate based on intention.

2. Weakening Encryption Harms Everyone's Security: If technology companies weaken encryption to allow government access, they weaken encryption for everyone. This means that the private banking information of millions of Americans, medical records, business secrets, and personal communications would all become vulnerable to attack. Criminals do not need government backdoors when the same weakness can be exploited for their own criminal purposes. To protect some, we would leave all vulnerable.

3. It Is Technically Impossible to Limit Access: Leading cryptography experts and computer scientists—including researchers from MIT, Columbia, Harvard, and Princeton—have concluded that it is technically impossible to create encryption systems with backdoors that only law enforcement can use. The mathematical reality is that any access mechanism can be misused or stolen. Creating a "master key" to encryption is like creating a key that works on every house in America—if the wrong person gets it, everything is at risk.

4. International Complications and Human Rights Violations: If the United States requires backdoors in encryption, authoritarian governments like China, Russia, and North Korea will demand the same access. Technology companies would be forced to choose between following U.S. law and following demands from repressive governments. This would enable mass surveillance in countries where human rights are violated. Journalists, political activists, and ordinary citizens in oppressed countries could be arrested or killed if their encrypted communications were exposed to authoritarian regimes.

Public Forum Debate Topic (NSDA, Nov-Dec 2025)

Resolved: *The U.S. should require technology companies to provide lawful access to encrypted communications.*

CON: REJECTING LAWFUL ACCESS TO ENCRYPTED COMMUNICATIONS (Continued...)

5. Protects Vulnerable Populations: Encryption protects people who are most vulnerable to government abuse and surveillance. Domestic violence victims use encrypted apps to communicate safely with shelters and counselors. Immigrants in dangerous situations use encryption to protect themselves. People reporting government corruption use encryption to stay safe. LGBTQ individuals in oppressive regions rely on encryption to protect their identity. Weakening encryption harms all of these vulnerable people.

6. Law Enforcement Has Alternative Methods: Computer scientists argue that law enforcement has many tools available that do not require weakening encryption for everyone. Police can use metadata analysis (studying who called whom and when), advanced data analytics, improved hacking techniques on individual devices, lawful hacking to exploit vulnerabilities, international cooperation, and better training for investigators. These alternatives are being used successfully today and can be improved without sacrificing everyone's security.

7. History Shows Government Power Gets Abused: Throughout history, governments have abused surveillance powers. The FBI illegally wiretapped civil rights leaders including Dr. Martin Luther King Jr. The government has secretly surveilled journalists, activists, and ordinary citizens. Microsoft documented thousands of government gag orders hiding searches of citizens' data. If the government has tools for surveillance, it has repeatedly shown a tendency to use them beyond their original purpose, often without proper oversight.

8. Criminals Will Simply Use Different Encryption: Requiring access to commercial encryption services will not stop sophisticated criminals and terrorists. Criminals can use open-source encryption software that is freely available on the internet. They can use encryption tools created in other countries. They can develop their own encryption. Bad actors will always have access to strong encryption regardless of what law is passed. Only law-abiding citizens would be forced to use weakened encryption.

9. There Is No Emergency Justifying This Action: The data shows that the encryption problem is manageable. Law enforcement encounters encryption regularly, but they still successfully investigate and prosecute the vast majority of cases. Law enforcement has better tools and more data available today than ever before. Surveys show that encryption is used in fewer than one percent of criminal cases that go unsolved. There is no crisis requiring that we sacrifice everyone's security.

10. Strong Encryption Enables Good Things: Encryption protects people's freedom of speech, freedom of conscience, and freedom of association. It allows doctors to communicate confidentially with patients, lawyers to protect attorney-client communications, and businesses to keep trade secrets safe. Encryption enables people to participate in democracy without fear. If we weaken encryption, we lose all of these benefits for millions of people, affecting far more people than the crimes law enforcement wants to investigate.