LAWFUL ACCESS TO ENCRYPTED DATA ACT

SPONSORED BY CONGRESSWOMAN ANN WAGNER

The Fourth Amendment to the Constitution balances a citizen's reasonable expectation of privacy with society's legitimate need to access evidence in order to protect the public from criminal actors. The *Lawful Access to Encrypted Data Act* is a balanced solution that protects the constitutional rights of all Americans while providing law enforcement with the tools they need to access evidence necessary to address violent crime and national security threats.

The legislation would require service providers and device manufacturers to assist law enforcement in accessing encrypted data and devices after a court issues a warrant based on probable cause that a crime has been committed. The bill would incentivize technological innovation through a prize competition for solutions that allow lawful access in encrypted environments while ensuring maximum privacy and security for citizens. The bill would also fund training for law enforcement personnel on accessing digital evidence.

THE PROBLEM

Encryption technology is an important tool for safeguarding data and promoting cybersecurity. However, bad actors exploit "warrant-proof" forms of encryption to shield dangerous and illegal activities from legitimate law enforcement investigation. These crimes include human trafficking, child sexual abuse, drug trafficking, terrorism, and numerous others. Increasingly, service providers and device manufacturers are refusing to cooperate with law enforcement in accessing encrypted evidence, even when issued a warrant supported by probable cause. Without this assistance, investigations into some of the most serious crimes affecting our communities around the country are substantially frustrated, delayed, or even prevented entirely. This puts our communities and our national security at risk.

Coronavirus lockdowns have substantially heightened risks for children who are targeted online for sexual exploitation. Victims of exploitation and their families have pleaded with service providers, device manufacturers, and other technology companies to take responsible steps to make sure their platforms are not abused by bad actors. But many of these companies continue to prioritize profits and the absolute privacy of abusers over the safety, security, and privacy of children. This market failure allows criminals to operate with impunity and must be corrected through legislative action.

During a Senate Judiciary Committee hearing in 2019, Manhattan District Attorney Cyrus Vance argued that as the technology industry evolves, the law must evolve with it. This has been the case throughout American history. When private sector harms that cannot—or will not—be addressed by industry are identified, Congress must act to preserve public safety. In the communications industry, Congress passed the Communications Assistance for Law Enforcement Act to preserve wiretapping capability; in the financial services industry, Congress required banks to adopt systems to detect money laundering and provide data to law enforcement; in the pharmaceutical industry, Congress passed laws requiring manufacturers to go through an FDA process to ensure drugs were safe; in the agriculture industry, Congress passed the Pesticide Control Amendment of 1954 establishing safety limits; and in the construction industry, Congress passed the Clean Air Act of 1970 to protect Americans from asbestos exposure. This is government's role when an industry cannot police itself and is exposing Americans to danger. Similarly, as the technology industry evolves, the *Lawful Access to Encrypted Data Act* would ensure law enforcement can still properly investigate and prosecute criminal activity while maintaining the privacy rights of Americans.

CONGRESSWOMAN
ANN WAGNER
2nd District of Missouri

THE SOLUTION: *LAWFUL ACCESS TO ENCRYPTED DATA ACT*

The *Lawful Access to Encrypted Data Act* balances consumer privacy with public safety and includes three components:

LAWFUL ACCESS

- Mandates service providers and device manufacturers to provide assistance, pursuant to a warrant and appropriate legal process, required to recover encrypted information stored on a device, operating system, or remote computing service, or access encrypted information in transit over a wire or electronic communication service.
- Authorizes the Attorney General to issue directives to service providers and device manufacturers to report on technical capabilities to comply with court orders and timelines for developing and deploying those capabilities.
    - The Attorney General may not specify the technical means needed to implement the required capabilities.
    - Anyone issued a directive may petition a federal court to set aside the directive by proving by clear and convincing evidence that it is scientifically impossible to comply with the directive, or that the directive is otherwise unlawful.
    - DOJ would be responsible for compensating anyone subject to a directive for reasonable expenses incurred in complying with the directive.

PRIZE COMPETITION

- Provides $50 million authorization for the Attorney General to design a prize competition to incentivize creative technological innovation in developing lawful access solutions in encrypted technology, while maximizing privacy and security.

LAWFUL ACCESS TRAINING

- Authorizes $50 million, contingent on solicitations matching the authorization amount, to create a training program and real-time assistance for law enforcement personnel at the National Domestic Communications Assistance Center (NDCAC).

SUPPORTING ORGANIZATIONS

National Association of Police Organizations
Major Cities Chiefs Association
National Association of Assistant U.S. Attorneys
Major County Sheriffs of America
National District Attorneys Association
Association of State Criminal Investigative Agencies
National Center of Sexual Exploitation
Stop Child Predators
Sergeant's Benevolent Association
Federal Law Enforcement Officers Association
U.S. Institute Against Human Trafficking
Share Hope International
National Sheriffs Association

WHAT THEY ARE SAYING
ABOUT THE *LAWFUL ACCESS TO ENCRYPTED DATA ACT*

- *Ed Mullins, President of Sergeants Benevolent Association of the New York City Police Department:* "**The 'Lawful Access to Encrypted Data Act' strikes this necessary balance and will ensure that service providers and device manufacturers provide all necessary assistance and develop the appropriate technology to both ensure adequate protection of privacy and public safety.** The SBA is proud to join you in advocating for passage of this legislation, and we thank you for your continued leadership on this important issue."
- *William Johnson, Executive Director of the National Association of Police Organizations:* "Digital evidence is a part of nearly every crime scene today and law enforcement is increasingly facing real and growing challenges in getting this evidence when we obtain the required legal process. This significantly hampers law enforcement's ability to keep our communities safe, prosecute criminals and protect victims… **The Lawful Access to Encrypted Data Act will ensure that when law enforcement is investigating such heinous crimes as kidnapping, homicide, child pornography or human trafficking, service providers must assist us in obtaining that information for the investigation.**"
- *Chief Art Acevedo, President of Major Cities Chiefs Association:* "The MCCA fully recognizes the benefits encryption affords to law abiding citizens. **The right to privacy that Americans enjoy is part of what makes our country great. However, we cannot let criminals continue their malicious use of this technology at the expense of our communities' safety**… The MCCA believes that the Lawful Access to Encrypted Data Act strikes the proper balance between lawful access and privacy."
- *Lawrence. J. Leiser, President of the National Association of Assistant United States Attorneys:* "Currently, criminals are able to hide behind outdated data privacy laws that threaten public safety. **The Lawful Access to Encrypted Data Act addresses this gap in enforcement by codifying into federal law a requirement that technology companies ensure federal law enforcement have a process for obtaining lawful access to encrypted data**… NAAUSA fully endorses this legislation to bypass longstanding obstacles to achieving justice."
- *Peter J. Koutoujian, President of the Major County Sheriffs of America:* **"Your legislation would create very reasonable requirements for companies to comply with legal orders pursuant to search warrants**… That is why we support your bill and will work to educate all Members of the Senate and House about its importance to our agencies and the citizens we serve."
- *Duffie Stone, President of the National District Attorneys Association:* "The introduction of the Lawful Access to Encrypted Data Act reflects the immediate need for a legislative solution to the issue of smartphone device encryption and lawful access to digital evidence. **By accounting for detailed processes that require a valid warrant and court order, while also accounting for the resources needed to ensure that technology community is able to comply with these orders, your legislation represents a realistic path forward to solving this complicated problem."**
- *Mark Keel, President of the Association of State Criminal Investigative Agencies:* "ASCIA understands that strong encryption is an essential part of modern cybersecurity. We also believe that tradeoffs have always been a part of system design. A lawful access mechanism that balances system security against the very real public safety harm caused by warrant-proof encryption is consistent with long-standing tradeoffs in other areas of system design, like the need for software updates**. Your bill strikes an appropriate balance and we commend your recognition of the seriousness of this issue**."
- *Benjamin Bull, General Counsel for the National Center on Sexual Exploitation:* "Encryption, while valuable for user privacy, provides a mechanism for child predators to operate anonymously and with impunity. As a result, **the Internet has become a law-enforcement-free-zone for predators and traffickers. This bill is necessary to ensure that law enforcement can take reasonable, and constitutional measures to investigate crimes and protect children while respecting individual privacy.**"

- *Stacie Rumenap, President of Stop Child Predators:* "'The Lawful Access to Encrypted Data Act' strikes the right balance between privacy and effective law enforcement. **Stop Child Predators applauds efforts to protect against dangerous criminal activity, which often includes putting vulnerable children at great risk, while at the same time respecting civil liberties. Privacy and protection don't have to be mutually exclusive, and this bill reasonably accounts for both.**"
- *Larry Cosme, President of the Federal Law Enforcement Officers Association:* "Digital evidence is the new smoking gun of 21st Century law enforcement. Whether in terrorism, child porn or a fraud case, today's evidence is always tied to a digital platform - of which private companies hold the key to but often won't turn it**. It is long overdue that private companies in the digital world be mandated to help law enforcement and comply with lawful court orders - and the 'Lawful Access to Encrypted Data Act' is a step toward ensuring those companies are finally mandated to help law enforcement protect America."**
- *Kevin Malone, Chairman of the Board of the U.S. Institute Against Human Trafficking:* "Passage of the 'Lawful Access to Encrypted Data Act' would provide law enforcement with the necessary resources to effectively investigate and prosecute cases of human trafficking and child sexual exploitation, while also protecting the individual citizen's reasonable expectation of privacy… **We thank you for your leadership in introducing the 'Lawful Access to Encrypted Data Act' and will actively encourage members of the U.S. House to advance this legislation to provide the necessary tools for law enforcement to effectively combat the systematic buying and selling of America's most vulnerable citizens**."
- *Congresswoman Linda Smith, Founder and President of Shared Hope International (1995-99):* "Shared Hope International is deeply concerned about the costs to victims of child sex trafficking and sexual exploitation when encryption policies proceed without consideration or accountability for the impact on crime victims. The proliferation of online criminal activity involving children requires a robust dialogue and creative solutions to find technological approaches that allow for lawful access to critical information. This access is essential to prevent traffickers and exploiters from using encryption to shield their illegal activities from law enforcement. **Shared Hope International sees the Lawful Access to Encrypted Data Act as a critical step to ensuring encryption does not create barriers to law enforcement's efforts to protect children online.**"
- *Sheriff Vernon Stanforth, National Sheriffs' Association 2nd Vice President:* "For far too long, law enforcement has been stymied by criminals who hide their wrongful acts on their electronic devices**. This legislation has the necessary elements to protect ordinary citizen's privacy and help law enforcement keep communities safe. It would allow courts, in support of a duly authorized search warrant, based on probable cause, to search an electronic device with compelled third party assistance. With these crucial safeguards in place, The National Sheriffs Association supports the measure**."

CONGRESSWOMAN
ANN WAGNER
2nd District of Missouri