

Take Action

Internet Society Open Letter Against Lawful Access to Encrypted Data Act

July 7, 2020

The Honorable Lindsey Graham
Chairman, Senate Committee on the Judiciary

The Honorable Marsha Blackburn
Senate Committee on the Judiciary

The Honorable Tom Cotton
Senate Committee on the Judiciary

Dear Senators Graham, Blackburn, and Cotton:

The undersigned organizations and security experts from civil society, industry and academia express our strong opposition to the Lawful Access to Encrypted Data Act, S. 4051. The bill's language as drafted is seriously flawed and could endanger public and national security.

The bill would expose millions of Americans—and people around the world who use American products and services—to substantially higher risk from malicious cyber actors, including hostile states and cyber criminals. This bill would require companies to build encryption backdoors. In some cases this would be by default. In others, backdoors would be linked to nine new or expanded requirements for companies or people to comply with government demands for “technical assistance” in law enforcement investigations. The definitions of “technical assistance” explicitly include “decrypting” information. Thus the bill’s requirements are so broad that it would effectively force recipients to build and maintain encryption backdoors to provide the data when requested. Such requirements would seriously weaken security; as highlighted by experts, including former senior national security and law enforcement officials, in the Carnegie Endowment for International Peace’s 2019 report **[Moving the Encryption Policy Conversation Forward](#)**.

The bill’s flawed premise is evident in its findings. As currently written, it states that strong encryption is dangerous and it facilitates “criminal activity,” without acknowledging that end-to-end encryption protects all people and is vital to many sectors of the economy, from banking to healthcare. Further, the bill’s findings fail to recognize the magnitude of vulnerability it would create for hundreds of millions of Americans who rely on strong encryption every day of their lives, especially as the global pandemic shifts much of their lives online.

Interviews with hundreds of federal, state, and local law enforcement officials have shown that the largest barrier to law

enforcement when dealing with modern communications systems is not encryption. Rather, it is an inability to leverage the data they currently have or *could* have access to. The intent of the Lawful Access to Encrypted Data Act may be to promote public safety, but regardless of how law enforcement or legislators attempt to require exceptional access to encrypted communications, the result is the same: it would put the safety and security of Internet users in danger at a moment when a devastating pandemic has made secure technologies more critical than ever to the everyday lives of Americans.

In addition, this effort will threaten the widespread adoption of strong encryption, which is essential for protecting the national security of the United States and the confidentiality, integrity, and availability of important data for all persons, corporations, and other organizations, including governmental actors.

Why Encryption Matters

Strong encryption is vital for national security, the economy, personal security and safety, individual liberty, and free expression. Encryption allows individuals to freely express themselves, to exchange personal and other sensitive information, and to protect their data. This includes active duty military personnel stationed overseas, scientists, doctors and patients, attorneys, journalists, human rights workers abroad, political campaigns, corporate executives, and victims of domestic abuse and other vulnerable communities.

Strong, unfettered encryption is vital to national and personal

security. Individuals, businesses, and governments—including law enforcement, national security agencies, military personnel, and government officials—use the same commercial off-the-shelf (“COTS”) encrypted services to ensure that the content of their communications is protected against outside surveillance or malicious modification.

Encrypted services are also vital to the U.S. economy—large sectors including online banking, e-commerce, and R&D rely on trusted encrypted services. Encrypted services are even more important now, during the COVID-19 pandemic, for remote working, learning, and healthcare. Removing, weakening or disincentivizing the use of strong encryption, as this bill effectively does, would threaten our economy and sacrifice all users’ security and privacy, leaving their communications, financial transactions, health information, and other data susceptible to misuse by bad actors, including the military and intelligence services of hostile states, organized criminals, terrorist groups, domestic abusers, and malicious hackers.

Backdoors to encryption make everyone in society more vulnerable to cybersecurity threats, privacy violations, foreign government surveillance, and other risks. Any backdoor will inevitably be leaked or discovered and used by malicious actors.

A backdoor for law enforcement is a backdoor for bad actors as well.

Conclusion

Preventing crime and keeping people safe is a universal priority—and is also the ultimate goal of the use of encryption technologies. Making everyone more vulnerable to criminals, malicious actors, and foreign intelligence services would be the unfortunate impact of passing the Lawful Access to Encrypted Data Act. It is too technically flawed to be effective, and will force companies to make their products less secure.

We support the goal of promoting public safety, but the Lawful Access to Encrypted Data Act would have the opposite effect, and it would compromise Americans' security. Therefore, we strongly oppose this bill.

Sincerely,

Civil Society Organizations

Access Now

Advocacy for Principled Action in Government

Center for Democracy and Technology

Defending Rights & Dissent

Derechos Digitales

Electronic Frontier Foundation (EFF)

Fight for the Future

Global Partners Digital

Human Rights Watch

Internet Society

Internet Users Forever IKI

LGBT Technology Partnership

National Coalition Against Censorship

PEN America

Prostasia Foundation

Restore the Fourth

SFLC.in

Swathanthra Malayalam Computing

TechFreedom

The Tor Project

Wikimedia Foundation

World Wide Web Consortium (W₃C)

Technology Companies and Trade Associations

ACT | The App Association

Afilias

Blacknight

Reform Government Surveillance

Ribose Inc.

Valimail

Security and Policy Experts*

Dr. Ben Adida, Executive Director, VotingWorks

Matt Anderson, Trust & Safety Specialist, Linode

Daniel Appelquist, co-chair of the W3C Technical Architecture Group and Director of Web Advocacy at Samsung Electronics

Anivar Aravind, Executive Director, Indic Project

Brian Behlendorf, The Linux Foundation

Steven M. Bellovin, Percy K. and Vida L.W. Professor of Computer Science and affiliate law faculty, Columbia University

Matt Bishop, Professor of Computer Science, University of California at Davis

Nathaniel Borenstein, Chief Scientist, Mimecast

Georgia Bullen, Executive Director, Simply Secure

Jon Callas, Senior Technology Fellow, ACLU

L. Jean Camp, Indiana University

Seth Blank, VP of Standards and New Technologies, Valimail

Stephen Checkoway, Assistant Professor of Computer Science,
Oberlin College

Sven Dietrich, City University of New York

Roger Dingledine, The Tor Project

Zakir Durumeric, Stanford University

David Evans, University of Virginia

Alexander Falatovich, Lead Cyber Security Threat Analyst

Alex Gouaillard, W3C AB representative for and CEO of
CoSMo Software

Alex Gaynor, Alloy

J. Alex Halderman, Professor of Computer Science and
Engineering; Director, Center for Computer Security and
Society, University of Michigan

Dr. Sven Herpig, Director for International Cybersecurity Policy,

Stiftung Neue Verantwortung

Chelsea Holland Komlo, University of Waterloo

Allen Householder, Senior Vulnerability Analyst, CERT/CC,
Software Engineering Institute, Carnegie Mellon University

J.C. Jones, Mozilla Corporation

Chris Kanich, University of Illinois at Chicago

Dr. Joseph Kiniry, Galois and Free & Fair

Dr. Peter Y. A. Ryan, University of Luxembourg

Petri Koistinen, Nitor

Susan Landau, Tufts University

Dave Lugo, Systems Engineer, Comcast

Art Manion, CERT/CC, Software Engineering Institute,
Carnegie Mellon University

Sascha Meinrath, Director, X-Lab, Palmer Chair in
Telecommunications, Penn State University

Peter G. Neumann, Chief Scientist, SRI International Computer
Science Lab, and moderator of the ACM Risks Forum

Zigmund J Ozea, Senior Programmer, Zetalytics

Jon M. Peha, Carnegie Mellon University

Riana Pfefferkorn, Stanford Center for Internet and Society

Ronald Rivest, Massachusetts Institute of Technology

Bruce Schneier, Lecturer, Harvard Kennedy School

Ross Schulman, New America's Open Technology Institute

Wendy Seltzer, Strategy Lead, World Wide Web Consortium (W3C)

Micah Sherr, Georgetown University

Adam Shostack, Shostack & Associates

Harold Solbrig, Johns Hopkins University

Ashkan Soltani, Georgetown University

Michael Alan Specter, Massachusetts Institute of Technology

Jonathan Spring, CERT/CC, Software Engineering Institute, Carnegie Mellon University

Venkat Venkatakrisnan, Professor, UIC

Dan S. Wallach, Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public Policy, Rice University

Nicholas Weaver, Researcher, ICSI & Lecturer, UC Berkeley

Daniel Zappala, Brigham Young University

Dr. Daniel M. Zimmerman, Galois and Free & Fair

Lenore D Zuck, Research Professor, University of Illinois at Chicago

**Affiliations provided for identification purposes only*

SIGN THE LETTER

We use cookies to ensure that we give you the best experience on our website. If you continue to use this site we will assume that you are okay with that.

Ok

Privacy policy