Hon. Brett Guthrie
Chair, House of Representatives Committee on Energy and Commerce

April 4, 2025

Hon. Frank Pallone
Ranking Member, House of Representatives Committee on Energy and Commerce

RE: Fix the TAKE IT DOWN Act to Protect Encryption

Dear Chair Guthrie and Ranking Member Pallone,

We, the undersigned civil society organizations and cybersecurity experts and academics, write to urge Congress to amend the TAKE IT DOWN Act, as passed by the Senate (S. 146), because it creates unacceptable risks to users' fundamental privacy rights and cybersecurity by undermining encryption. The bill is intended to address nonconsensual distribution of intimate imagery (NDII), which is profoundly harmful and violative of victims' privacy and autonomy. But those harms must be addressed in a manner that does not incentivize platforms to compromise cybersecurity or use invasive content monitoring technologies that diminish users' privacy and freedom of speech.

The right to private communications is a cornerstone of free speech, and today, private, secure communications are made possible by encryption. Encryption is a best practice in data privacy and security, protecting all Americans from undue surveillance and censorship.

The TAKE IT DOWN Act, through its notice and takedown mechanism and overbroad definition of "covered platform," presents an existential threat to encryption. Among its provisions, the Act requires covered platforms to remove reported NDII and "make reasonable efforts to identify and remove any known identical copies" within 48 hours of receiving valid requests.

Although the Act appropriately excludes some online services — including "[providers] of broadband internet access service" and "[electronic] mail" — from the definition of "covered platform," the Act does not exclude private messaging services, private electronic storage services, or other services that use encryption to secure users' data.

The consequences are severe: it could be impossible for providers of encrypted services to comply with the Act's obligations without breaking encryption and introducing systemic security flaws. This is because providers of encrypted services do not have access to the content that can be reported under the Act, which will incentivize them to break encryption or implement invasive content monitoring technologies to shield themselves from liability. Moreover, the Act does not explain what constitutes "reasonable efforts" to identify copies of NDII on a provider's platform, creating an incentive for providers to abandon encryption out of fear that abandonment is necessary to show such effort. Breaking encryption, and coercing providers to abandon it, jeopardizes all users' privacy and cybersecurity. In the context of the TAKE IT DOWN Act, this means exposing the data of hundreds of millions of Americans, including the data of the victims of NDII this Act intends to protect, to otherwise avoidable risks. During this period of heightened threat, as evidenced by the Salt Typhoon hack, these risks must not be tolerated.

To address the profound harms of NDII without undermining encryption, Congress should add private messaging services, private electronic storage services, and other services that are encrypted to the email exception that is already in the bill.

Thank you for your efforts to combat the spread of nonconsensual intimate imagery. We look forward to working with Congress to find solutions that do not come at the cost of fundamental privacy rights and cybersecurity. Please direct your response to this letter to John Perrino, senior policy and advocacy expert at the Internet Society, at perrino@isoc.org, or Ryan Polk, director of internet policy at the Internet Society, at polk@isoc.org.

Sincerely,

Civil society organizations:

Advocacy For Principled Action In Government

American Civil Liberties Union

Americans for Prosperity

Center for Democracy & Technology

Center for Online Safety and Liberty

Defending Rights & Dissent

Demand Progress Action

Electronic Frontier Foundation (EFF)

Electronic Privacy Information Center (EPIC)

Freedom of the Press Foundation

Internet Governance Project, *Georgia Tech School of Public Policy**

Internet Society

LGBT Tech

New America's Open Technology Institute

Organization for Identity & Cultural Development

Project for Privacy and Surveillance Accountability

Restore the Fourth

TechFreedom

Tech For Good Asia

The Tor Project

*Cybersecurity experts and academics:**

Abdirahman Farah, *University of Bosaso*

Adam Shostack, *author, Threat Modeling: Designing for Security*

Andy Sayler, PhD

Christopher Joseph, *SecureCrypt*

Eugene H. Spafford, *Professor, Purdue University*

Jon Callas, *Indiana University*

Joseph Lorenzo Hall, PhD, *Internet Society*

Masayuki Hatta, *Surugadai University*

Philip Zimmermann, *Associate Professor Emeritus, Cybersecurity Group, Delft University of Technology*

Riana Pfefferkorn, *Stanford University*

Roya Ensafi, *University of Michigan*

Susan Landau, *Tufts University*

Wendy Seltzer

*Affiliation is indicated for purposes of identification only.

cc: Members of the House Energy and Commerce Committee