



March 10, 2020

Sen. Lindsay Graham, Chairman
Sen. Dianne Feinstein, Ranking Member
Senate Judiciary Committee
Dirksen Senate Office Building 226
Washington DC 20515

Re: March 11 Hearing on the EARN IT Act

Dear Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

On behalf of Amnesty International (“Amnesty”), we submit this statement to express our serious concerns with the negative impact that the EARN IT Act will have on the rights to privacy and freedom of expression. While Amnesty fully supports responsible efforts to address the problem of child exploitation online, we are concerned that the EARN IT Act would lead to an encryption “backdoor,” which would in turn increase the risks that all Americans face online.

1. Why Encryption Is Critical for Human Rights

Encryption is an essential means of protecting all our personal information. While there are different kinds of encryption, they all aim to achieve the same thing: to ensure that information can only be accessed by its owner or its intended recipient.

States have obligations under international law to respect, protect and fulfil the right to privacy. In the digital age, these obligations mean that states should ensure the security of online communications, including by raising awareness of internet security issues, encouraging the identification and repair of security weaknesses in computer networks and systems, and facilitating the use of encryption tools and services.

The threats to our private data are real and growing. Millions of Americans have had their data stolen, including as the result of large data breaches of companies and

government agencies. Such data thefts are a threat to security and privacy. For instance, the five largest data breaches of 2019 resulted in 540.3 million records compromised, including personal usernames, email addresses and passwords.¹

As the Committee well knows, these attacks are not solely the work of non-state actors. Often other nation states are responsible. For instance, in December 2018 the U.S. Justice Department indicted two individuals associated with the Chinese Ministry of State Security for waging a decade-long “intrusion campaign” against U.S. Government agencies as well as more than 45 American technology companies.²

At the same time, the actions of the U.S. government have increasingly threatened and violated our right to privacy, through unjustified surveillance. For years, mass surveillance programs operated by intelligence agencies in the U.S. have operated in the shadows and spied on the telephone and internet communications of hundreds of millions of people around the world.

In addition, technology for targeted electronic surveillance has become widely available and affordable. In recent years evidence has surfaced of surveillance technology being used against human rights defenders in countries such as Bahrain, the United Arab Emirates and Mexico.³

In the digital age, access to and use of encryption is an essential component of the right to privacy. Encryption allows people to share their opinions with others without fear of

¹ Megan Leonhardt, *The 5 biggest data hacks of 2019*, CNBC, 17 December 2019, accessible at:

<https://www.cnn.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html>

² The United States Department of Justice, *Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, 20 December 2018, accessible at: <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>

³ *Scores of Activists Targeted with NSO Spyware on WhatsApp*, Amnesty International, October 29, 2019, accessible at: <https://www.amnestyusa.org/press-releases/scores-of-activists-targeted-with-nso-spyware-on-whatsapp/>

reprisals. It also allows people to access information and to organize, even under repressive regimes. Strong encryption is an essential component of the rights to freedom of expression, information, opinion, and peaceful assembly.⁴ Encryption is a particularly critical tool for human rights defenders, activists and journalists, all of whom rely on it with increasing frequency to protect their security and that of others against unlawful surveillance.⁵ According to Zeid Ra'ad Al Hussein, the former UN High Commissioner for Human Rights: "It is neither fanciful nor an exaggeration to say that, without encryption tools, lives may be endangered. In the worst cases, a government's ability to break into its citizens' phones may lead to the persecution of individuals who are simply exercising their fundamental human rights."⁶

2. The Impact of the EARN IT Act on Encryption

The EARN IT Act mandates the creation of a National Commission on Online Child Exploitation Prevention (the "Commission"). According to the Act, "The purpose of the Commission is to develop recommended best practices for providers of interactive computer services regarding the prevention of online child exploitation conduct."⁷

⁴ *Encryption: A Matter of Human Rights*, Amnesty International, March 2016, accessible at:

https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

⁵ Cynthia Wong, *Why Encryption Back Doors Threaten Human Rights*, Human Rights Watch, July 8, 2015, accessible at: <https://www.hrw.org/news/2015/07/08/why-encryption-back-doors-threaten-human-rights>

⁶ Office of the UNH High Commissioner for Human Rights, *Apple-FBI case could have serious global ramifications for human rights: Zeid*, 4 March 2016, accessible at:

<http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf>

⁷ Earn It Act, Section 3(b), accessible at: <https://assets.documentcloud.org/documents/6746282/Earn-It.pdf>

The Commission is charged with “develop[ing] and submit[ing] to the Attorney General recommended best practices regarding the prevention of online child exploitation conduct.” The Attorney General will then “review, and modify if necessary, the recommended best practices, and publish a final version of the best practices on the website of the Department of Justice and in the Federal Register.” Companies must then annually certify that they comply with these best practices, or risk the loss of protections under Section 230 of the Communications Decency Act.

We are concerned that the Commission would mandate the creation of encryption “backdoors,” which would allow law enforcement agencies access to encrypted communications. Under Section 4 of the Act, setting forth the duties of the Commission, there are few limits on what constitute “best practices,” and no requirement that the Commission refrain from endorsing encryption backdoors. We are not alone in this concern.

According to a letter submitted to the Committee on March 6, 2020 and signed by 25 civil society organizations: “The Department of Justice has made no pretense about its desire to force online platforms to eliminate strong encryption technologies. The bill affords so much law enforcement control over the guidelines the Commission would produce, that it would provide officials a mechanism for pressuring small and large online service providers to eliminate strong encryption under threat of losing Section 230 protections.”⁸

3. Encryption Backdoors Constitute a Significant Interference with the Right to Privacy and Freedom of Expression

Amnesty International set out our recommendations on encryption backdoors in 2016.⁹ We recognize that strong encryption can pose challenges to accessing information for

⁸ *Coalition Letter Opposing EARN IT*, March 6, 2020

⁹ *Encryption: A Matter of Human Rights*, Amnesty International, March 2016, accessible at: https://www.amnestyusa.org/wp-content/uploads/2017/04/encryption_-_a_matter_of_human_rights_-_pol_40-3682-2016.pdf

legitimate law enforcement purposes. Governments have an obligation to protect their populations from crime, including exploitation, and electronic surveillance can be legitimately used for this purpose, if undertaken within the bounds of international law.

However, in attempting to overcome the barriers that encryption poses to them, state authorities must not violate the rights to privacy and freedom of expression, or any other rights for which the security of electronic data and communications is vital.

Amnesty believes that broad restrictions on access to and use of encryption undermine the rights to privacy and freedom of expression. As such, in order to avoid violating their human rights obligations, states must ensure that any restrictions on encryption are contained in laws that are precise and transparent, are used only when necessary to achieve a legitimate aim and do not discriminate against specific individuals or groups.

Critically, any interference with encryption must be proportionate to achieving the legitimate aim for which it is imposed, and the benefits gained must not be outweighed by the harm caused, including to individuals and network infrastructure and security.


4. Conclusion

Forcing companies to provide ‘backdoors’ to the encryption deployed in their products or services (potentially affecting all users) constitutes a significant interference with users’ rights to privacy and freedom of expression. Given that such measures indiscriminately affect all users’ online privacy by undermining the security of their electronic communications and private data, Amnesty believes that they are inherently disproportionate and thus impermissible under international human rights law.

For the reasons set forth above, we urge you to amend the EARN IT Act, to explicitly bar the Commission from mandating that companies create an encryption backdoor or otherwise weaken encryption protections.

For more information, please contact Joanne Lin, National Director for Advocacy and Government Affairs, at 202/509-8151 or jlin@aiusa.org.

Sincerely,

A handwritten signature in black ink, appearing to read "Joanne Lin". The signature is fluid and cursive, with the first name "Joanne" written in a larger, more prominent script than the last name "Lin".

Joanne Lin
National Director
Advocacy and Government Affairs Amnesty International USA

A handwritten signature in black ink, appearing to read "Michael Kleinman". The signature is highly stylized and cursive, with a long horizontal line extending to the right from the end of the name.

Michael Kleinman
Director, Silicon Valley Initiative
Amnesty International USA