19 August 2021

Tim Cook
CEO, Apple, Inc.

Dear Mr. Cook:

The undersigned organisations committed to civil rights, human rights and digital rights around the world are writing to urge Apple to abandon the plans it announced on 5 August 2021 to build surveillance capabilities into iPhones, iPads and other Apple products. Though these capabilities are intended to protect children and to reduce the spread of child sexual abuse material (CSAM), we are concerned that they will be used to censor protected speech, threaten the privacy and security of people around the world, and have disastrous consequences for many children.

Apple announced that it is deploying a machine learning algorithm to scan images in its text messaging service, Messages, to detect sexually explicit material sent to or from people identified as children on family accounts. This surveillance capability will be built right into Apple devices. When the algorithm detects a sexually explicit image, it warns the user that the image may be sensitive. It also sends a notice to the organiser of a family account whenever a user under age 13 chooses to send or to receive the image.

Algorithms designed to detect sexually explicit material are notoriously unreliable. They are prone to mistakenly flag art, health information, educational resources, advocacy messages, and other imagery. Children's rights to send and receive such information are protected in the U.N. Convention on the Rights of the Child. Moreover, the system Apple has developed assumes that the "parent" and "child" accounts involved actually belong to an adult who is the parent of a child, and that those individuals have a healthy relationship. This may not always be the case; an abusive adult may be the organiser of the account, and the consequences of parental notification could threaten the child's safety and wellbeing. LGBTQ+ youths on family accounts with unsympathetic parents are particularly at risk. As a result of this change, iMessages will no longer provide confidentiality and privacy to those users through an end-to-end encrypted messaging system in which only the sender and intended recipients have access to the information sent. Once this backdoor feature is built in, governments could compel Apple to extend notification to other accounts, and to detect images that are objectionable for reasons other than being sexually explicit.

Apple also announced that it would build into the operating system of its products a hash database of CSAM images provided by the National Center for Missing and Exploited Children in the United States and other child safety organisations. It will scan against that database every photo its users upload to iCloud. When a preset threshold number of matches is met, it will disable the account and report the user and those images to authorities. Many users routinely

upload the photos they take to iCloud. For these users, image surveillance is not something they can opt out of; it will be built into their iPhone or other Apple device, and into their iCloud account.

Once this capability is built into Apple products, the company and its competitors will face enormous pressure -- and potentially legal requirements -- from governments around the world to scan photos not just for CSAM, but also for other images a government finds objectionable. Those images may be of human rights abuses, political protests, images companies have tagged as “terrorist” or violent extremist content, or even unflattering images of the very politicians who will pressure the company to scan for them. And that pressure could extend to all images stored on the device, not just those uploaded to iCloud. Thus, Apple will have laid the foundation for censorship, surveillance and persecution on a global basis.

We support efforts to protect children and stand firmly against the proliferation of CSAM. But the changes that Apple has announced put children and its other users at risk both now and in the future. We urge Apple to abandon those changes and to reaffirm the company’s commitment to protecting its users with end-to-end encryption. We also urge Apple to more regularly consult with civil society groups, and with vulnerable communities who may be disproportionately impacted by changes to its products and services.

Sincerely,

Access Now (Global)
Advocacy for Principled Action in Government (United States)
African Academic Network on Internet Policy (Africa)
AJIF (Nigeria)
American Civil Liberties Union (United States)
Aqualtune Lab (Brasil)
Asociación por los Derechos Civiles (ADC) (Argentina)
Association for Progressive Communications (APC) (Global)
Barracón Digital (Honduras)
Beyond Saving Lives Foundation (Africa)
Big Brother Watch (United Kingdom)
Body & Data (Nepal)
Canadian Civil Liberties Association
CAPÍTULO GUATEMALA DE INTERNET SOCIETY (Guatemala)
Center for Democracy & Technology (United States)
Centre for Free Expression (Canada)
CILIP/ Bürgerrechte & Polizei (Germany)
Código Sur (Centroamerica)
Community NetHUBs Africa
Dangerous Speech Project (United States)
Defending Rights & Dissent (United States)
Demand Progress Education Fund (United States)

Derechos Digitales (Latin America)
Digital Rights Foundation (Pakistan)
Digital Rights Watch (Australia)
DNS Africa Online (Africa)
Electronic Frontier Foundation (United States)
EngageMedia (Asia-Pacific)
Eticas Foundation (Spain)
European Center for Not-for-Profit Law (ECNL) (Europe)
Fight for the Future (United States)
Free Speech Coalition Inc. (FSC) (United States)
Fundación Karisma (Colombia)
Global Forum for Media Development (GFMD) (Belgium)
Global Partners Digital (United Kingdom)
Global Voices (Netherlands)
Hiperderecho (Peru)
Instituto Beta: Internet & Democracia – IBIDEM (Brazil)
Instituto de Referência em Internet e Sociedade - IRIS (Brazil)
Instituto Liberdade Digital - ILD (Brazil)
Instituto Nupef (Brazil)
Internet Governance Project, Georgia Institute of Technology (Global)
Internet Society Panama Chapter
Interpeer Project (Germany)
IP.rec - Law and Technology Research Institute of Recife (Brazil)
IPANDETEC Central America
ISOC Bolivia
ISOC Brazil - Brazilian Chapter of the Internet Society
ISOC Chapter Dominican Republic
ISOC Ghana
ISOC India Hyderabad Chapter
ISOC Paraguay Chapter
ISOC Senegal Chapter
JCA-NET (Japan)
Kijiji Yeetu (Kenya)
LGBT Technology Partnership & Institute (United States)
Liberty (United Kingdom)
mailbox.org (EU/DE)
May First Movement Technology (United States)
National Coalition Against Censorship (United States)
National Working Positive Coalition (United States)
New America's Open Technology Institute (United States)
OhmTel Ltda (Columbia)
OpenMedia (Canada/United States)
Paradigm Initiative (PIN) (Africa)
PDX Privacy (United States)

PEN America (Global)
Privacy International (Global)
PRIVACY LATAM (Argentina)
Progressive Technology Project (United States)
Prostasia Foundation (United States)
R3D: Red en Defensa de los Derechos Digitales (Mexico)
Ranking Digital Rights (United States)
S.T.O.P. - Surveillance Technology Oversight Project (United States)
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Sero Project (United States)
Simply Secure (United States)
Software Freedom Law Center, India
SWOP Behind Bars (United States)
Tech for Good Asia (Hong Kong)
TEDIC (Paraguay)
Telangana (India)
The DKT Liberty Project (United States)
The Sex Workers Project of the Urban Justice Center (United States)
The Tor Project (Global)
UBUNTEAM (Africa)
US Human Rights Network (United States)
WITNESS (Global)
Woodhull Freedom Foundation (United States)
X-Lab (United States)
Zaina Foundation (Tanzania)