14 April 2022

Re: The Online Safety Bill

Dear Parliamentarian,

As technologists, security experts and NGOs, committed to the protection of digital rights around the world, we are writing to urge you to resist the UK Government's plans to create new powers to surveil the messages of citizens in the United Kingdom. We are concerned that these extraordinary capabilities will cause significant, irreversible damage to people's right to private communications and could, in the future, be both upscaled and imitated to censor protected speech and threaten privacy and security across other international jurisdictions.

In particular, we wish to bring attention to clause 103(2)(b) of the Online Safety Bill which provides the UK communications regulator, OFCOM, with the powers to order a provider of a user-to-user service, which includes private messaging platforms, "to use accredited technology" to identify child sexual exploitation and abuse (CSEA) content, including on private messaging platforms. However, in doing so, these notices could require that providers of such services introduce scanning capabilities into their platforms to scan all user content. Such scanning cannot be accomplished on end-to-end encrypted services for the simple reason that nobody, including the provider, has access to the content carried on that service except for the sender and the intended recipient(s). As a result, such a requirement could put users at risk by compelling their service providers to compromise or abandon end-to-end encryption.

We agree that more must be done to tackle pernicious CSEA content online. It is important to note that law enforcement agencies in the UK already possess a wide range of powers to seize devices, compel passwords and even covertly monitor and hack accounts to overcome security measures and identify criminals.

As has been widely documented by human rights groups and security experts, including recently in relation to a proposal by Apple to introduce scanning capabilities into its devices, scanning technologies "are notoriously unreliable and prone to mistakenly flag art, health information, educational resources, advocacy messages, and other imagery". Apple later retracted this proposal due to the inherent risks to privacy and security that would have arisen from the implementation of such a policy. Far from protecting children, such a requirement would compel providers of services, both large and small, to introduce vulnerabilities into their platforms that jeopardise not only device security but place the rights of all users, including children, at grave risk.

Privacy and safety are mutually reinforcing concepts. As signatories from all over the world, we have serious concerns that these steps from a liberal democracy such as the UK would not only harm people in the UK but set a bad precedent for other governments to follow. This measure opens up the possibility of similar approaches being taken to infiltrate private communications channels for other purposes both in the UK and around the world, including to further violate human rights.

Moreover, this requirement would constitute a departure from long standing legal standards, designed to protect freedom of speech and privacy online. For these reasons, we call for the clause to be dropped in its entirety.

The proposal is ill-suited to address its stated aim and instead places huge risk to all users of private messaging platforms, as well as creating unimplementable and impractical requirements which would be at odds with human rights standards.

Yours faithfully,

Access Now
Alec Muffett, Security Researcher
ARTICLE 19: Global Campaign for Free Expression
Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
Bangladesh NGOs Network for Radio and Communication
Big Brother Watch
Center for Democracy and Technology (CDT)
Canadian Civil Liberties Association
Christian de Larrinaga FBCS CITP
Committee to Protect Journalists (CPJ)
Dr. Christopher Parsons, Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto (affiliation provided for identification only)
Državljan D / Citizen D
Dr Douwe Korff, Emeritus Professor of International Law
Global Partners Digital (GPD)
Digitalcourage
Digitale Gesellschaft
Foundation for Information Policy Research
Homo Digitalis
Kijiji Yeetu
Georgia Tech Internet Governance Project (Atlanta USA)
Internet Society Catalan Chapter (ISOC-CAT)
Internet Society Brazil Chapter (ISOC Brazil)
Internet Society India Delhi Chapter
Internet Society India Hyderabad Chapter
Internet Society
Internet Society Portugal Chapter (ISOC PT)
Internet Society
IT-Pol Denmark
New America's Open Technology Institute
Open Rights Group
Praxonomy
Privacy & Access Council of Canada
Prof. Alan Woodward, Department of Computer Science, University of Surrey (affiliation provided for identification only)
Runa Sandvik, Security Researcher
Prof. Kapil Goyal, Observer, GIGANET, Academic Fellow, Alumni Fellow, inSIG, APSIG
Prof. Preeti Kamra, Alumni Fellow, VSIG , SSIG,
Ranking Digital Rights
Riana Pfefferkorn, Stanford Internet Observatory (affiliation provided for identification only)
CCAOI
Vaultree Limited
Simply Secure
Software Freedom Law Center, New York
SFLC.in (India)
Tech for Good Asia
Tresorit
Tutanota