Open Rights Group
The Society of Authors
24 Bedford Row
London, WC1R 4EH

European Digital Rights (EDRi)
Rue Belliard 12
1040 Brussels
Belgium

To: Chloe Smith, Secretary of State,
Department for Science, Innovation and Technology

cc: Tom Tugendhat, Minister of State for Security, Home Office
Paul Scully, Minister for Tech and the Digital Economy
Lord Parkinson of Whitley Bay

Dear Ms Smith,

Online Safety Bill: Civil society organisations urge UK to protect global digital security and safeguard private communication.

We are over 80 national and international civil society organisations, academics and cyber-experts. We represent a wide range of perspectives including digital human rights and technology. We are writing to you to raise our concerns about the serious threat to the security of private and encrypted messaging posed by the UK's proposed Online Safety Bill (OSB).

The Online Safety Bill is a deeply troubling legislative proposal. If passed in its present form, the UK could become the first liberal democracy to require the routine scanning of people's private chat messages, including chats that are secured by end-to-end encryption. As over 40 million UK citizens and 2 billion people worldwide rely on these services, this poses a significant risk to the security of digital communication services not only in the UK, but also internationally.

End-to-end encryption ensures the security of communications for everyone on a network. It is designed so that no-one, including the platform provider, can read or alter the messages. The confidentiality between sender and recipient is completely preserved. That's why the United Nations, several human rights groups, and anti-human trafficking organisations alike have emphasised that encryption is a vital human rights tool.[i]

In order to comply with the Online Safety Bill, platform providers would have to break that protection either by removing it or by developing work-arounds. Any form of work-around risks compromising the security of the messaging platform, creating back-doors, and other dangerous ways and means for malicious actors and hostile states to corrupt the system.[ii] This would put all users in danger.

The UK government has indicated its intention for providers to use a technology that would scan chats on people's phone and devices – known as client-side scanning. The UK government's assertion that client-side scanning will not compromise the privacy of messages contradicts the significant evidence of cyber-security experts around the world. This software intercepts chat messages before they are encrypted, and as the user is uploading their images or text, and therefore confidentiality of messages cannot be guaranteed. It would most likely breach human rights law in the UK and internationally.[iii]

---

i Human rights, encryption and anonymity in a digital age: report of the UN Special Rapporteur on freedom of expression: www.ohchr.org/en/stories/2015/06/human-rights-encryption-and-anonymity-digital-age
Encryption: a matter of human rights, Amnesty International: www.amnesty.org/en/documents/pol40/3682/2016/en/
Quotes from Polaris anti-trafficking project in news article: www.nbcnews.com/tech/tech-news/wickr-amazon-aws-child-messaging-app-sex-abuse-problem-rcna20674

ii Bugs in Our Pockets: The Risks of Client-Side Scanning: arxiv.org/abs/2110.07450

Serious concerns have also been raised about similar provisions in the EU's proposed 'Child Sexual Abuse Regulation', which an independent expert study warns is in contradiction to human rights rules.[iv] French, Irish and Austrian parliamentarians have all also warned of severe threats to human rights and of undermining encryption.[v]

Moreover, the scanning software would have to be pre-installed on people's phones, without their permission or full awareness of the severe privacy and security implications. The underlying databases can be corrupted by hostile actors, meaning that individual phones would become vulnerable to attack. The breadth of the measures proposed in the Online Safety Bill – which would infringe the rights to privacy to the same extent for the internet's majority of legitimate law-abiding users as it would for potential criminals – means that the measures cannot be considered either necessary or proportionate.[vi]

The inconvenient truth is that it is not possible to scan messages for bad things without infringing on the privacy of lawful messages. It is not possible to create a backdoor that only works for "good people" and that cannot be exploited by "bad people".

Privacy and free expression rights are vital for all citizens everywhere, in every country, to do their jobs, raise their voices, and hold power to account without arbitrary intrusion, persecution or repression. End-to-end encryption provides vital security that allows them to do that without arbitrary interference. People in conflict zones who rely on secure encrypted communications to be able to speak safely to friends and family as well as for national security. Journalists around the world who rely on the confidential channels of encrypted chat, can communicate to sources and upload their stories in safety.

Children, too, need these rights, as emphasised by UNICEF based on the UN Convention of the Rights of the Child.[vii] Child safety and privacy are not mutually exclusive; they are mutually reinforcing. Indeed, children are less safe without encrypted communications, as they equally rely on secure digital experiences free from their data being harvested or conversations intercepted. Online content scanning alone cannot hope to fish out the serious cases of exploitation, which require a whole-of-society approach. The UK government must invest in education, judicial reform, social services, law enforcement and other critical resources to prevent abuse before it can reach the point of online dissemination, thereby prioritising harm prevention over retrospective scanning.[viii]

As an international community, we are deeply concerned that the UK will become the weak link in the global system. The security risk will not be confined within UK borders. It is difficult to envisage how such a destructive step for the security of billions of users could be justified.[ix]

---

iii Internet Society, Client-side scanning: What it is and why it threatens trustworthy, private communication, May 2023, staging.internetsociety.org/wp-content/uploads/2020/04/Client-side-Scanning-Fact-Sheet-EN.pdf
Open Letter from Public Interest Technologists in relation to the European Commission's proposed Regulation on Child Sexual Abuse (CSA): www.politico.eu/wp-content/uploads/2023/05/10/Experts-letter-encryption-CSA.pdf
Safety Tech Challenge Fund Evaluation Report, see comments on human rights compliance p2: bpb-eu-w2.wpmucdn.com/blogs.bristol.ac.uk/dist/1/670/files/2023/02/Safety-Tech-Challenge-Fund-evaluation-framework-report.pdf

iv Civil Liberties Committee of the European Parliament and European Parliamentary Research Service (EPRS), Complementary Impact Assessment to the proposed EU Regulation laying down rules to prevent and combat child sexual abuse: www.europarl.europa.eu/RegData/etudes/STUD/2023/740248/EPRS_STU(2023)740248_EN.pdf

v Irish and French parliamentarians sound the alarm about EU's CSA Regulation: edri.org/our-work/irish-and-french-parliamentarians-sound-the-alarm-about-eus-csa-regulation/
Binding Resolution of the Austrian Parliament against the Child Sexual Abuse Regulation: epicenter.works/document/4393

vi Index on Censorship, Opinion from Matthew Ryder KC. Surveilled and Exposed: How the Online Safety Bill Creates Insecurity: www.indexoncensorship.org/wp-content/uploads/2022/11/Surveilled-Exposed-Index-on-Censorship-report-Nov-2022.pdf

vii Convention on the Rights of the Child, UNICEF: www.unicef.org/child-rights-convention/convention-text-childrens-version

viii CRIN: Privacy and Protection: A children's rights approach to encryption: home.crin.org/readlistenwatch/stories/privacy-and-protection; and Ross Anderson: Chat Control of Child Protection: www.lightbluetouchpaper.org/2022/10/13/chatcontrol-or-child-protection/

The UK Prime Minister, Rishi Sunak, has said that the UK will maintain freedom, peace and security around the world. With that in mind, we urge you to ensure that end-to-end encrypted services will be removed from the scope of the Bill and that the privacy of people's confidential communications will be upheld.

Signed,

Access Now
ARTICLE 19: Global Campaign for Free Expression
Asociația pentru Tehnologie și Internet (ApTI)
Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)
Association for Progressive Communications (APC)
Big Brother Watch
Centre for Democracy and Technology
Chaos Computer Club (CCC)
Citizen D / Državljan D
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Community NeHUBs Africa
cyberstorm.mu
Defend Digital Me
CASM at Demos
Digitalcourage
Digitale Gesellschaft
DNS Africa Media and Communications
Electronic Frontier Finland
Electronic Frontier Foundation (EFF)
Electronic Frontier Norway
Epicenter.works
European Center for Not-for-Profit Law
European Digital Rights (EDRi)
European Sex Workers Rights Association (ESWA)
Fair Vote
Fight for the Future
Foundation for Information Policy Research
Fundación Cibervoluntarios
Global Partners Digital
Granitt
Hermes Center for Transparency and Digital Human Rights
Homo Digitalis
Ikigai Innovation Initiative
Internet Society
Interpeer gUG
ISOC Brazil – Brazilian Chapter of the Internet Society
ISOC Ghana
ISOC India Hyderabad Chapter
ISOC Venezuela
IT-Pol
JCA-Net (Japan)
Kijiji Yeetu
La Quadrature du Net
Liberty
McEvedys Solicitors and Attorneys Ltd
Open Rights Group
OpenMedia
OPTF
Privacy and Access Council of Canada
Privacy International
Ranking Digital Rights
Statewatch
SUPERRR Lab
Tech for Good Asia
UBUNTEAM
Wikimedia Foundation
Wikimedia UK
Professor Paul Bernal
Nicholas Bohm
Dr Duncan Campbell
Alan Cox
Ray Corrigan
Professor Angela Daly
Dr Erin Ferguson
Wendy M. Grossman
Dr Edina Harbinja
Dr Julian Huppert
Steve Karmeinsky
Dr Konstantinos Komaitis
Professor Douwe Korff
Petr Kučera
Mark A. Lane
Christian de Larrinaga
Mark Lizar
Dr Brenda McPhail
Alec Muffett
Riana Pfefferkorn
Simon Phipps
Dr Birgit Schippers
Peter Wells
Professor Alan Woodward

---

ix See ii

x Rishi Sunak, Statement 14 March 2023: www.gov.uk/government/speeches/pm-statement-at-aukus-trilateral-press-conference