

Baroness Stowell
Chair, House of Lords Communications and Digital Committee
House of Lords
SW1A 0PW

13 December 2022

Dear Baroness Stowell,

Thank you for inviting us to speak at last week's committee hearing on the Online Safety Bill (the Bill).¹ During the hearing, we both mentioned to members that we would write to expand on our thoughts about the Online Safety Bill's expected effect on end-to-end encryption (E2EE). We hope this letter will help you and other committee members as you consider amendments to the Bill.

E2EE ensures that communication between users is indecipherable to third parties. Those snooping on E2EE services such as WhatsApp, Signal, and iMessage are unable to read the contents of the messages. This contrasts with email services such as Gmail and Short Message Services (SMS) used by mobile devices for texting, which do not encrypt content. Law enforcement and intelligence agencies can access the content of Gmail messages and texts sent via SMS.

E2EE services provide security and privacy to millions of law-abiding British citizens and residents.² UK citizens and businesses rely on E2EE to keep themselves safe and secure from frequent and sophisticated cyber attacks.³ It is critical for financial services, the health sector, and national security. Yet criminals also use E2EE services, making it harder for police to gather evidence. This feature of E2EE is a source of understandable frustration to police and those worried about the spread of content the Bill seeks to tackle.

As written, the Bill poses a threat to E2EE. Clause 106 would allow Ofcom to require a user-to-user service or a search service to "use accredited technology to identify CSEA [child sexual exploitation and abuse] content, whether communicated publicly or *privately* by means of the service, and to swiftly take down that content." (emphasis added).⁴

Encrypted services such as WhatsApp and Signal are user-to-user services as defined by the Bill.⁵ As such, Ofcom could compel them to use accredited technology to find and remove CSEA content on their platforms. E2EE makes such search and removal impossible. If the Bill is passed without amendment, the most likely scenario is that services providing E2EE would modify their service and deploy a controversial technology called client-side scanning (CSS) to comply with notices issued by Ofcom.⁶ Leading cybersecurity experts have argued convincingly that message scanning, mistakenly

¹ <https://committees.parliament.uk/event/15985/formal-meeting-oral-evidence-session/>

² For example, nearly 75 percent of UK internet users use WhatsApp, <https://www.statista.com/statistics/284506/united-kingdom-social-network-penetration/>

³ <https://www.gov.uk/government/news/businesses-urged-to-boost-cyber-standards-as-new-data-reveals-nearly-a-third-of-firms-suffering-cyber-attacks-hit-every-week>

⁴ C.106 <https://publications.parliament.uk/pa/bills/cbill/58-03/0209/220209.pdf>

⁵ "In this Act 'user-to-user service' means an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service" c .2(1)

⁶ <https://www.indexoncensorship.org/2022/11/new-legal-opinion-on-the-online-safety-bill/>

considered safe and effective by its proponents, “creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic.”⁷

We believe that the integrity of E2EE is crucial not only for the confidentiality and privacy of communications but also for moral and essential cybersecurity reasons. Researchers have provided solid evidence that compromising E2EE compromises the network security and safety of the same users we wish to protect.⁸

The specific amendment we support would entail **leaving out the word ‘privately’ in clause 106, lines 35 and 39**. We urge you to consider and adopt this amendment. Members of Parliament have previously recommended such an amendment as well as explicit protection for E2EE services.⁹

Thank you for considering the risks to E2EE posed by the Bill. We would both welcome the opportunity to discuss the risks further with you and any of your colleagues.

Sincerely,

Matthew Feeney
Head of Technology & Innovation, Centre for Policy Studies

Dr Edina Harbinja
Reader in law, Aston University

⁷ <https://arxiv.org/abs/2110.07450>

⁸ <https://arxiv.org/abs/2210.08958>

⁹ NC 38. https://publications.parliament.uk/pa/bills/cbill/58-03/0121/amend/onlinesafety_day_rep_0712.pdf
#153. https://publications.parliament.uk/pa/bills/cbill/58-03/0121/amend/onlinesafety_rm_rep_0715.pdf