Comments of the Global Encryption Coalition Steering Committee on Ofcom's 9 November 2023 Consultation: Protecting People from Illegal Harms Online

Submitted 23 February 2024 via email to Ofcom at IHconsultation@ofcom.org.uk

These non-confidential comments are submitted on behalf of the Global Encryption Coalition's Steering Committee, which consists of the Center for Democracy & Technology, Global Partners Digital, the Internet Freedom Foundation, the Internet Society, and the Mozilla Corporation. They concern the Draft Guidance Ofcom prepared regarding implementation of the UK Online Safety Act, with a focus of Volume 2 of the Guidance (causes of online harm) and Volume 4 (mitigating the risk of illegal harms).

While Ofcom recognizes that encryption is an important security measure, this recognition is weak and understates the societal value of encryption, and in particular, its value for promoting cybersecurity in an increasingly risky environment. It also gives short shrift to the value that encryption provides for children as it can often shield them from harm. We believe that Ofcom ought to promote a more balanced approach that properly accounts for the benefits of encryption. This is the approach that the European Court of Human Rights took just last week when it rejected the imposition of backdoors to encryption in the case of *Podchasov v Russia*. Indeed, encryption is a valuable tool in addressing some of the risks that Ofcom says it poses. For example, end-to-end encryption (E2EE) protects users against fraud as it secures messages so that only the sender and the intended recipients can access the contents of the communication, making them less vulnerable to fraud than they would be if their unsecured message was intercepted by a fraudster. A service that is unsecured by E2EE is riskier from the perspective of fraud prevention than a service that is secured by E2EE. The Guidance should recognize this, as well as the extent to which E2EE provides security against other societal ills with respect to which at present the Guidance solely identifies encryption as a risk factor.

Moreover, the Guidance stresses alleged risks that E2EE poses in a variety of contexts that are unrelated to combating Child Sexual Exploitation and Abuse (CSEA), sending a mixed message to the services secured by E2EE about their duty to scan for illegal content. Under the Online Safety Act (OSA), CSEA is the only societal ill with respect to which there may be imposed a duty to scan for illegal content on user-to-user (U2U) services that are encrypted. Yet, Ofcom's list of risks to be addressed goes well beyond CSEA. As a result, providers that protect the public and children by offering communications services that are encrypted end-to-end are guided toward regarding themselves as "high risk" on account of risks relating not to CSEA, but to "hate crime, terrorism, drugs, immigration, sexual offences, extreme pornography, intimate image abuse, proceeds of crime, fraud, foreign interference and false communications".

Listing end-to-end encryption as a risk factor suggests that there are actions that providers can take to mitigate this risk. At the same time, the OSA restricts Ofcom's power to require the use of proactive content moderation technologies within encrypted environments, except for Child

Sexual Exploitation and Abuse (CSEA) material. Ofcom's framing of encryption as a risk factor places indirect pressure on providers, effectively circumventing the limitations for E2EE laid out in the OSA. Ofcom's framing implicitly pushes service providers not to roll-out encryption on their services.

Instead, Ofcom should clarify that the risk factor, according to which measures should be adopted, is the risk of the use of a U2U service that is encrypted for the purpose of exchanging CSEA. The Guidance should also clarify that with respect to that risk, Ofcom will not require E2EE services to adopt measures such as client-side scanning. This is required because the duty to adopt proactive measures does not apply when such adoption is not technically feasible without compromising the security of a service.

There is more than ample evidence that client-side scanning would indeed compromise the security of E2EE services, as shown in particular by this report, Bugs in Our Pockets, produced by noted computer security experts. They point out that a client-side scanning requirement to address the risks posed by CSEA would introduce the type of security vulnerabilities that the OSA prohibits Ofcom from requiring. Other research, including a study by the European Parliament Research Service regarding the proposed EU CSAM regulation confirms that currently there are no technically feasible means of allowing access to content on systems that are encrypted end-to-end without compromising the security of the system as a whole. Client-side scanning can be insufficiently accurate at detecting CSEA, result in false positives, and be vulnerable to "poisoning attacks" on hash databases used in detection efforts. The draft Guidance properly restricts the use of hash matching to detect CSEA to content that is publicly communicated, but encryption is missing as a factor to consider when determining whether content was communicated publicly or privately.

The Global Encryption Coalition Steering Committee recommends that Ofcom remove E2EE as a risk factor within risk assessments, and that the Guidance be revised in Annex 9 to make it clear that encryption is a factor in determining whether content should be regarded as having been communicated privately.

[Questions about these non-confidential comments of the Global Encryption Coalition Steering Committee may be directed to Greg Nojeim, Director of the Security and Surveillance Project at the Center for Democracy & Technology, gnojeim@cdt.org.]