# Open Rights Group's '48 hours to tell Ofcom: Practice safe text' campaign

Shortly before the closing date for responses to our consultation, the Open Rights Group (ORG) launched a campaign called '48 hours to tell Ofcom: Practice safe text' ('the Campaign'). This was part of a wider Practice Safe Text campaign that was launched by the ORG in February 2025. The Campaign stated:

> ***'The vital cybersecurity tool of end-to-end encryption is under threat. Here's why:***
>
> *Ofcom are currently running a consultation on their framework for implementing the 'Spy Clause' section 121 of the Online Safety Act (https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/consultation-technology-notices/) This clause gives Ofcom the power to issue a technical notice to a provider, and require them to use a specific technology to scan everyone's messages for terrorist material or child sexual exploitation materials (CSEM).*
>
> ***This consultation closes at 5pm on Monday 10th March 2025.***
>
> *The problem is there is no safe scanning technology that exists. Many of the imagined solutions (such as client-side scanning) could create major security risks for the UK and our allies.'*

The Campaign encouraged the public to read and respond to our consultation 'to warn Ofcom of the risks involved by implementing unsafe scanning tech' and to tell Ofcom to 'practice safe text and back end-to-end encryption'.

The campaign was published on the ORG website and was later shared on their social media accounts. It recommended the public read our consultation and write their own reply to Ofcom. However, the ORG's website also provided a tool that could be used to submit an automated response using a template, which could be sent directly or edited within the tool before submitting. Responses to our consultation via the tool were sent/received from an ORG email address unique to each individual respondent.

The template consultation response was as follows:

> *I wish to respond to the following consultation question."*
>
> *'Do you have any views on our audit-based assessment, including our proposed principles, objectives, and the scoring system? Please provide Evidence to support your response.'*
>
> *It is my view that Ofcom needs to consider how it scores and considers the following risks and threats that could arise from accrediting any scanning technologies:*
>
> *1. The threat that the system might infringe on people's human right to free expression or privacy. This is particularly relevant given these systems could break end-to-end encryption and the recent ECHR ruling in the case of Podchasov v. Russia – https://hudoc.echr.coe.int/eng/?i=001-230854. Ofcom will have a legal duty to assess the proportionality of any such system that doesn't infringe on our human rights. It could find*

*itself facing legal challenges over this issue if it doesn't demonstrate an assessment of the impact on the right to privacy from breaking E2EE within its framework.*

*2. The risk of false positives & wrongful accusations. If these are too high then law enforcement agencies will be flooded with false positive results from any scanning system and people will be wrongfully accused, causing them harms. A higher threshold should therefore be applied to accuracy.*

*3. The risks are that any system will break UK data protection laws and/or undermine the nation's cybersecurity by introducing backdoor vulnerabilities to private and secure messaging systems. The recent situation where Apple has withdrawn its advanced data protection product from the UK market highlights that forcing or approving a poor technology upon a company could result in UK users losing access to products. Ofcom should consider the risks to UK consumers of forcing new technologies onto providers that are not feasible to deliver or have too high economic and social costs.*

*4. Equalities act implications and impact on people with protected characteristics. Ofcom will have to consider the impact of any scanning system in relation to the public sector equalities duty.*

*5. Higher weighting in framework around risks where there are legal duties. The current minimum threshold for 'fairness' does not consider the risk Ofcom faces of breaking its legal obligations to consider the Human Rights Act, Equalities Act and the Data Protection Act. As such a separate scoring and risk assessment should be taken for each technology it considers to ensure Ofcom can evidence it has met its statutory legal duties.*

*6. The risk any system will facilitate the spread of CSEM. A regulator wishing to control the use of image-based sexual abuse (IBSA) removal tools must carefully assess the risks posed by perceptual hash inversion attacks. These attacks could result in someone creating CSEM images from the hashed data that the tool was using. For evidence of these attacks, see S. Hawkes, C. Weinert, T. Almeida and M. Mehrnezhad, "Perceptual Hash Inversion Attacks on Image-Based Sexual Abuse Removal Tools," in IEEE Security & Privacy, doi: 10.1109/MSEC.2024.3485497. Further risks and threats from scanning technologies are set out in 'Bugs in our pockets: the risks of client-side scanning - Harold Abelson, Ross Anderson, Steven M Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G Neumann, Ronald L Rivest, Jeffrey I Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso, Bugs in our pockets: the risks of client-side scanning, Journal of Cybersecurity, Volume 10, Issue 1, 2024, tyad020, https://doi.org/10.1093/cybsec/tyad020"*

When our consultation closed on 10 March 2025, Ofcom had received 782 responses submitted via the Campaign tool. 629 responses matched the template consultation response. 94 responses paraphrased the pre-prepared text or included additional sentences added by individual respondents to the template consultation response. The majority of these additional sentences reflected the professional capacity in which the individual was responding or endorsed the benefits of end-to-end encryption.

The remaining 59 responses were unique responses that did not use the template consultation response. The following are themes that were mentioned most frequently:

a) **The potential infringement of human rights, including the rights to data protection, privacy, freedom of expression and association.** A number of responses highlighted potential adverse impacts of scanning systems on particular groups that rely on end-to-

end encrypted communication. These include individuals with protected characteristics (e.g., women, LGBTQIA+ individuals, individuals with disabilities) or vulnerable populations (e.g., domestic abuse survivors, people in care, individuals experiencing tech-facilitated abuse), as well as academics, activists, and journalists.

b) **The risk of creating vulnerabilities which can be exploited by malicious actors**. Several respondents warned that "backdoors" designed for legitimate purposes could be exploited by bad actors, including criminals, hostile state actors, and hackers. This could result in the UK being vulnerable to cyberattacks and undermine global cybersecurity. The U.S government's endorsement of end-to-end-encrypted services following the Salt Typhoon attack was cited as an example of why encryption should be preserved in light of attacks by hostile state actors.

c) **The potential risk of mission creep and surveillance by authorities.** A number of respondents noted the potential risk of authorities repurposing mass scanning systems for surveillance purposes. They noted that this would lead to curtailment of civil liberties and set a global precedent for other countries to follow.

d) **The risk of false positives and the impact of wrongful accusations on individuals.** Respondents emphasised that mass scanning systems can generate false positives, overwhelming law enforcement and potentially leading to wrongful accusations that are detrimental to individuals. The British Post Office Horizon IT scandal was cited as a notable example of the damaging impact wrongful accusations can have.

e) **Impacts on competition, innovation for technology providers, and consumer choice.** Some respondents noted that mandating certain technologies could hinder competition and innovation by deterring smaller companies from entering the market and in existing products being withdrawn from the market. This would in turn lead to UK consumers being placed at a disadvantage as they would have fewer choices.

f) **Need for independent oversight and operational accountability.** Respondents stated the need for transparency, independent oversight, clear mechanisms for redress, and auditable processes to ensure biases are identified and corrected when operationalising Technology Notices. Additionally, respondents noted Ofcom's obligations to consider the Human Rights Act, Equality Act, and Data Protection Act in its assessment of proportionality.

In addition to these common themes, responses also noted:

- The risk of driving illegal activity into unofficial networks, which can lead to the creation of alternative channels of communication that are unregulated and harder to monitor.
- The potential for selective data usage and algorithmic biases to adversely impact specific groups disproportionately, further entrenching existing inequalities and leading to discriminatory outcomes.
- Challenges around implementing content detection technologies on open-source messaging applications as users can disable features, block reports, or manipulate the systems.
- The requirement for continuous updates for technologies to ensure long-term viability as technologies and cyber threats evolve rapidly.
- The need to focus on improving law enforcement capabilities within existing legal frameworks and improve detection mechanisms that do not compromise encryption.
- The need to encourage voluntary cooperation from service providers while preserving security standards.

- The risks posed by mandated backdoors resulting in a weakening of public trust in secure communications, financial, and business transactions.
- The need to consider international regulatory differences and cross-border implications when implementing these technologies.
- The need to support educational initiatives about online safety.
- That the weakening of encryption is seen as a threat to democracy and public trust.