Your response

Question	Your response
Question 1: 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	N/A
Question 2: Do you have any views on our proposals for independent performance testing, including the two mechanisms for setting thresholds; the approach to testing technologies in categories against particular metrics; and data considerations? Please provide evidence to support your response.	As an organisation offering support to survivors of gender-based violence (GBV), Chayn[1] has serious concerns about The Technical Notice regime proposed under this consultation. First, the minimum standards of accuracy for accredited technologies are too low, and as such, could obligate service providers to integrate unreliable technologies into their systems. Given the number of global services that transmit millions or even billions of messages per day, and the technical impracticability of limiting the deployment of these technologies only to UK users, the contemplated accuracy standards may inadvertently undermine online safety by flooding reporting agencies like NCA with false positives, and/or forcing providers to commit significant resources and expertise to identifying false positives, such as by conducting extensive human review, that would have otherwise been invested in developing and maintaining more effective

[1] Chayn's work https://org.chayn.co/

	safety measures. Additionally - and most crucially for Chayn - the low accuracy threshold would introduce material risks to the privacy of abuse victims and survivors in particular. There are a wide range of reasons why GBV survivors may want or need to share graphic content related to their abuse online, such as preserving or sharing evidence of abuse with legal counsel, law enforcement, or support services and networks; and using encrypted online messaging services to find assistance, community, and heal.[2] The low accuracy threshold proposed in this consultation could lead to survivors' communications being wrongly flagged by accredited technologies and then subjected to invasive human review or improperly reported to third parties.
Question 3: Do you have any comments on what Ofcom might consider in terms of how long technologies should be accredited for and how often technologies should be given the opportunity to apply for accreditation? Is there any further evidence we should consider?	N/A
Question 4: Do you have any views on how to turn these proposals into an operational accreditation scheme, including the practicalities of submitting technology for accreditation? Is there any additional evidence that you think we should consider? Please provide any information that may be relevant.	Chayn believes that the accreditation scheme proposed does not provide sufficient safeguards to ensure that Technology Notices will not introduce significant new cybersecurity risks for users. For example, the Internet Society's technical feasibility assessment for content

[2] *See, e.g.,* Chayn's Bloom Notes tool that uses an end-to-encrypted messaging platform to share weekly messages with subscribers about the content of our Bloom courses, including references to trauma, healing, sex, and relationships: https://bloom.chayn.co/subscription/whatsapp. *See also,* end-to-end encrypted communications options for contacting support services like Scotland's Domestic Abuse and Forced Marriage Helpline: https://www.sdafmh.org.uk/en/.

	monitoring on end-to-end encrypted services in the context of the OSA concluded that “such measures compromise the integrity of devices and systems, increasing the risk of system-wide attacks and unauthorized access to personal data, whether accidental or malicious.”[3]
Question 5: Do you have any comments on our draft Technology Notice Guidance?	While we understand that this consultation does not take a view on scenarios that could threaten end-to-end encrypted environments, we nevertheless want to stress that if providers of encrypted services are required to develop or adopt third party tools with functions that report flagged content back to the service provider or to a third party, such as the NCA or law enforcement, that would be the technical and functional equivalent of requiring an encryption backdoor for data in transit. Enabling third party access to the plaintext of encrypted data in motion is widely considered to be so dangerous that Carnegie’s Encryption Working Group, made up of intelligence, law enforcement, and cryptography experts, concluded that it “would represent a fundamental weakening of all the communications.”[4] In light of the unique ways that GBV survivors rely on end-to-end encrypted services to access help, support, and safety, any Technology Notice that undermined or jeopardized the security and integrity of of those communications tools would in turn jeopardize the safety and privacy of

[3] Internet Society, Preemptive Monitoring in End-to-End Encrypted Services: A Technical Feasibility Evaluation (June 2024), https://www.internetsociety.org/wp-content/uploads/2024/07/Preemptive-Monitoring-in-E2EE-Services.pdf.

[4] Carnegie Endowment for International Peace, Encryption Working Group, Moving the Encryption Conversation Forward, pg. 10 (2019), https://carnegie-production-assets.s3.amazonaws.com/static/files/EWG__Encryption_Policy.pdf.

	individuals and service providers in this community. GBV survivors are indeed particularly at risk of unintended harmful impacts from the minimum standards of accuracy for accredited technologies and how Ofcom proposes to exercise its Technical Notice (TN) functions under the OSA. Survivors rely on secure technology to communicate with trusted contacts, contact service providers and other organisations that can provide help and support, and search for shelters or other resources in their area. This increased reliance on technology also makes them more vulnerable to online abuse, stalking, and harassment. They disproportionately benefit from broad safety and security technologies such as end-to-end encrypted messaging, and being confident in the security and efficacy of any content scanning and reporting tools that service providers are required to develop or adopt via the proposed accreditation scheme. Without strong digital security tools, abusers can and will leverage vulnerabilities against their victims.[5] Please find in the annex below a full response to the consultation.

Please complete this form in full and return to technologynotices@ofcom.org.uk

[5] Orbits: a global field guide to advance intersectional, survivor-centred, and trauma informed interventions to TGBV, pg. 60 (2022): https://c.chayn.co/orbits

Annex: Chayn's submission to the UK Government′s consultation on the Technology Notices to deal with terrorism content and/or CSEA content

Who are we?

Chayn is a UK-registered charity. We are a global organisation creating resources to support the healing of survivors of gender-based violence (GBV). Our focus is on empowering women and other marginalized genders who have experienced domestic, sexual or tech facilitated gender based violence (TFGBV). We create open, online resources and services for and with survivors of abuse that are trauma-informed, intersectional, multilingual and feminist. Technology is at the core of what we do. We use technology to provide support to survivors of GBV, we create feminist tech and explore feminist applications of existing technology. Much of this technology is designed with survivors of abuse from diverse experience and backgrounds. We are there to respond and support survivors of TFGBV. We use our expertise and experience to inform policy makers about the dangers of TFGBV.[6]

Why Chayn is responding to this consultation

As a service provider for survivors of GBV, the right to privacy is one of our core principles. Privacy is a fundamental right. Not only do survivors face high risks to their life, but also due to stigma, victim blaming, and shame associated with gender-based violence, the need for privacy is even greater for the people we support. This is why we see encryption, and end-to-end encryption in particular, not just as a privacy-preserving technology but as a feminist technology.[7]

We believe that weakening or removing end-to-end encryption exposes survivors to several risks:

- **Exposure of Private Communications:** Without encryption, personal messages can be intercepted, potentially revealing sensitive information about a survivor's location, plans, or support networks.
- **Retaliation from Abusers:** If abusers gain access to a survivor's communications, it can lead to increased harassment, manipulation, or physical harm.
- **Creates barriers in seeking support:** Fear of surveillance may deter survivors from reaching out for support, leaving them isolated and vulnerable.

[6] Chayn's work https://org.chayn.co/

[7] Orbits: a global field guide to advance intersectional, survivor-centred, and trauma informed interventions to TGBV, pg. 60 (2022): https://c.chayn.co/orbits

- **Compromised Safety Plans:** Survivors often develop detailed plans to escape abusive situations. Without secure communication, these plans can be discovered and thwarted by abusers.
- **Increased Surveillance:** Abusers may exploit weakened encryption to monitor survivors' activities, limiting their autonomy and freedom.
- **Loss of Trust in Support Services:** If confidentiality cannot be guaranteed, survivors may hesitate to engage with support services, legal advisors, or healthcare providers.

Chayn is therefore deeply concerned about the potential impact of the Technical Notices which Ofcom may issue to providers of end-to-end encrypted services under the Online Safety Act 2023 (OSA) on the safety and well-being of GBV survivors . We support the critical work that Ofcom does to promote public safety and protect vulnerable individuals and communities online.

Ofcom serves a critical role in ensuring online service providers adopt a wide range of practices and product features to keep their users safe, while also protecting fundamental rights like privacy and freedom of expression by limiting obligations to adopt specific tools and features under the OSA to those which satisfy the standards of necessity and proportionality.

However, we are concerned that the Technical Notice regime proposed in the current consultation **does not** strike the right balance, and may jeopardise access to security tools and practices that domestic and gender based violence victims rely on to keep them safe, including privacy preserving technologies and product features like end-to-end encryption and timely software/security updates.

Furthermore, as a global organisation, we strongly believe in the importance of establishing strong principles and best practices internationally when it comes to privacy and technology. As some governments ban encryption and access communications with no safeguards, it is essential for the UK to act as a leader in the protection of fundamental rights and the promotion of privacy enhancing technologies.

Unique concerns for survivors of gender-based violence

GBV survivors are particularly at risk of unintended harmful impacts from the minimum standards of accuracy for accredited technologies and how Ofcom proposes to exercise its Technical Notice (TN) functions under the OSA.

Survivors rely on secure technology to communicate with trusted contacts, contact service providers and other organisations that can provide help and support, and search for shelters or other resources in their area. This increased reliance on technology also makes them more vulnerable to online abuse, stalking, and harassment. They disproportionately benefit from broad safety and security technologies such as end-to-end encrypted messaging, and being confident in the security and efficacy of any content scanning and reporting tools that service providers are required to develop or adopt via the proposed accreditation scheme. Without strong digital security tools, abusers can and will leverage vulnerabilities against their victims.[8]

The importance of encryption for women is a reality that has been highlighted in different reports of UN commissioners and special rapporteurs. In a report from 2017, the United Nations High Commissioner for Human Rights, noted that "Women's right to privacy in the context of equal access to ICTs implies the ability to benefit from encryption, anonymity or the use of pseudonyms on social media in order to minimize the risk of interference with privacy, which is especially pertinent for women human rights defenders and women trying to obtain information otherwise considered taboo in their societies."[9]
In a report from 2021, the UN Special Rapporteur on freedom of expression states that "anonymity and the use of encryption and other privacy protocols are an essential facet of women's enjoyment of freedom of opinion and expression in the online context and must be protected."[10]

The Technical Notice regime proposed under this consultation raises serious concerns for GBV survivors.

First, the minimum standards of accuracy for accredited technologies are too low, and as such, could obligate service providers to integrate unreliable technologies into their systems. Given the number of global services that transmit millions or even billions of messages per day, and the technical impracticability of limiting the deployment of these technologies only to UK users, the contemplated accuracy standards may inadvertently undermine online safety by flooding reporting agencies like NCA with false positives, and/or forcing providers to commit significant resources and expertise to identifying false positives, such as by conducting extensive human review, that would have otherwise been invested in developing and maintaining more effective safety measures.

Additionally, the low accuracy threshold would introduce material risks to the privacy of abuse victims and survivors in particular. There are a wide range of reasons why GBV survivors may want or need to share graphic content related to their abuse online, such as preserving or sharing evidence of abuse with legal counsel, law enforcement, or support services and networks; and using encrypted online messaging services to find assistance, community, and heal.[11] The low accuracy threshold proposed in this

[8] *ibid.*

[9] Report of the United Nations High Commissioner for Human Rights, *Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective* https://documents.un.org/doc/undoc/gen/g17/111/81/pdf/g1711181.pdf.

[10] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan https://documents.un.org/doc/undoc/gen/n21/212/16/pdf/n2121216.pdf.

[11] *See, e.g.,* Chayn's Bloom Notes tool that uses an end-to-encrypted messaging platform to share weekly messages with subscribers about the content of our Bloom courses, including references

consultation could lead to survivors' communications being wrongly flagged by accredited technologies and then subjected to invasive human review or improperly reported to third parties.

Second, the accreditation scheme proposed does not provide sufficient safeguards to ensure that Technology Notices will not introduce significant new cybersecurity risks for users. For example, the Internet Society's technical feasibility assessment for content monitoring on end-to-end encrypted services in the context of the OSA concluded that "such measures compromise the integrity of devices and systems, increasing the risk of system-wide attacks and unauthorized access to personal data, whether accidental or malicious."[12]

Moreover, if providers of encrypted services are required to develop or adopt third party tools with functions that report flagged content back to the service provider or to a third party, such as the NCA or law enforcement, that would be the technical and functional equivalent of requiring an encryption backdoor for data in transit. Enabling third party access to the plaintext of encrypted data in motion is widely considered to be so dangerous that Carnegie's Encryption Working Group, made up of intelligence, law enforcement, and cryptography experts, concluded that it "would represent a fundamental weakening of all communications."[13]

In light of the unique ways that DV and GBV survivors rely on end-to-end encrypted services to access help, support, and safety, any Technology Notice that undermined or jeopardized the security and integrity of of those communications tools would in turn jeopardize the safety and privacy of individuals and service providers in this community.

Recommendations

Prioritising the safety of survivors through the use of encryption and ensuring high accuracy standards for any accredited technologies will help ensure that domestic and gender based violence survivors can safely access the support they need. We urge Ofcom to carefully consider these concerns and work towards creating a safer and more secure environment for all. Security is safety, and encryption is one of the best tools available to promote and ensure the security of our communities' communications.

As such, we believe that the Guidance should be amended to ensure that Ofcom:

- Cannot issue TNs that could undermine encryption; and.

to trauma, healing, sex, and relationships: https://bloom.chayn.co/subscription/whatsapp. *See also,* end-to-end encrypted communications options for contacting support services like Scotland's Domestic Abuse and Forced Marriage Helpline: https://www.sdafmh.org.uk/en/.

[12] Internet Society, Preemptive Monitoring in End-to-End Encrypted Services: A Technical Feasibility Evaluation (June 2024), https://www.internetsociety.org/wp-content/uploads/2024/07/Preemptive-Monitoring-in-E2EE-Services.pdf.

[13] Carnegie Endowment for International Peace, Encryption Working Group, Moving the Encryption Conversation Forward, pg. 10 (2019), https://carnegie-production-assets.s3.amazonaws.com/static/files/EWG__Encryption_Policy.pdf.

- Only accredits technologies that meet high standards of accuracy.