15 September 2026

IWF written evidence - The Online Safety Act: implementation and impact

1. Summary

1.1. The Internet Watch Foundation (IWF) welcomed the passage of the Online Safety Act (OSA), which established a long-needed regulatory floor for tackling online child sexual exploitation and abuse (CSEA). It remains too early to assess the overall impact of the legislation on keeping children safe online but there are encouraging signs that the OSA is beginning to drive meaningful change. In particular, the uptake of hash-matching and Ofcom's enforcement activity are helping to increase the proactive detection and blocking of known child sexual abuse material (CSAM), thereby reducing the spread of this content and preventing revictimisation. The rollout of highly effective age assurance (HEAA) across major pornography services is also creating important barriers for children's access to age-inappropriate content. Therefore, whilst implementation and enforcement of the OSA have been slower than anticipated, it remains a powerful piece of legislation.

1.2. The Online Safety Act still has the potential to transform children's safety online, provided the remaining barriers to meeting its full ambition are addressed. The IWF remain particularly concerned by the lack of safeguards for end-to-end encrypted (E2EE) environments. Government and Ofcom must start to remedy this by requiring services to introduce privacy-preserving methods, such as upload prevention, to detect and block known child sexual abuse material (CSAM). We also believe the OSA's technical feasibility condition and safe harbour provision are limiting its effectiveness by allowing services to avoid their safety duties on E2EE environments. Greater clarity is needed on how technical feasibility is assessed, and the safe harbour provision should be removed.

1.3. More broadly, the regulation of artificial intelligence remains a significant gap in the online safety regime. Government must ensure AI companies adopt a safety-by-design approach that identifies and mitigates harm from the outset. We also believe the current implementation of safety by design does not reflect Parliament's intent. The OSA should be amended to include a statutory definition of safety by design and a dedicated Code of Practice.

1.4. Finally, while some measures to address violence against women and girls (VAWG) have been introduced, women and girls continue to experience disproportionate levels of online harm. There is currently limited evidence of the measurable impact the OSA has had on improving outcomes for women and girls.

2. About the Internet Watch Foundation

2.1. The Internet Watch Foundation is an international not-for-profit organisation working closely with the global technology sector to disrupt, prevent and remove images and videos showing the sexual abuse and exploitation of children from digital spaces. We operate Europe's largest centre for assessing, grading and securing the removal of online child sexual abuse material.

2.2. The IWF provides trusted services, intelligence and datasets used by technology companies, platforms, financial and other industries, and law enforcement worldwide. These capabilities support safety-by-design approaches that help protect victims and survivors, prevent the spread of criminal content, and strengthen the global investigation and disruption of abuse networks.

3. Inquiry questions

3.1. **What evidence, if any, is there that children are safer online since the OSA protection of children duties came into force?**

3.1.1. The Online Safety Act has established important minimum standards for technology companies operating in the UK and has introduced new duties intended to ensure that children are protected from online harms. The introduction of enforceable duties to protect children from illegal and harmful content provides a stronger regulatory basis for safeguarding than what had previously existed in the UK. For example, the implementation of highly effective age assurance by pornography providers represents an important step towards preventing children from accessing harmful and age-inappropriate content. We discuss the impact of HEAA further in section 3.2.

3.1.2. However, the full capability of the Online Safety Act remains to be actualised, and it may therefore be too early to make a definitive assessment of its overall impact on children's safety online.

3.2. **What evidence, if any, is there that UK users are less exposed to illegal content and activity since the OSA illegal content duties came into force?**

3.2.1. As we mention in section 3.1, although the full capability of the OSA has not yet been actualised, this does not detract from the fact that it is a powerful piece of legislation. The Act has established minimum standards for technology companies operating in the UK and has introduced levers through which they can be held accountable in a way that they could not previously. This includes the need to proactively detect and block CSAM, which represents significant progress in tackling the spread, and recirculation, of content depicting the sexual abuse of children.

3.2.2. Since the Illegal Harms Codes came into force on 17 March 2025, Ofcom has launched an enforcement programme into file-storage and file-sharing services to prevent users from encountering CSAM. File-storage and file-sharing services are at greater risk of

being exploited by offenders to share CSAM at scale, and it is therefore vital that they implement hash-matching to block known child sexual abuse imagery.[1 & 2] The file-sharing and file-storage enforcement programme has also supported four services into adopting perceptual hash-matching .[3, 4, 5 & 6] Hash matching plays a crucial part in detecting known images of child sexual abuse and in turn reduces the risk of revictimisation for victims and survivors. Hash matching is central to combatting the spread of CSAM by providing highly accurate and privacy-preserving methods of detection.[7]

3.2.3. The launch of investigations into these services has resulted in six out of seven of them making their services unavailable to UK users.[8] It has also resulted in Ofcom issuing a provisional notice of contravention and fine of £20,000 to a particularly high-risk service.[9]

3.2.4. This is important and much needed progress as it means that companies are taking concrete steps to prevent their services from being exploited to share sexual abuse of children or preventing UK users from accessing this content. Whilst the pace of enforcement is slower than we had anticipated, it still a clear signal that the OSA is beginning to ensure the UK becomes a hostile environment for child sexual abuse material.

3.2.5. Additionally, the IWF has a growing user base of platforms citing OSA obligations, as one of the driving forces behind implementing Image Intercept into their systems. Image Intercept is IWF's free hash checking provided to support smaller platforms to proactively detect and block CSAM. Since its launch in July 2025 Image Intercept has scanned over 38,494,619 images and 3,076,792 video content around the world. This has resulted in over 73,923 images and videos of CSAM being blocked on these services.

---

[1] Ofcom (2025). File-storage and file-sharing: know the online safety risks, the rules, and how to comply [web].
[2] IWF (2026). Ofcom and IWF reinforce partnership in fight against online child sexual abuse [news].
[3] Ofcom (2026). Enforcement programme into measures being taken by file-sharing and file-storage services to prevent users from encountering or sharing child sexual abuse material (CSAM) [web]. See update on April 2026.
[4] Ofcom (2025). Wojtek's compliance assurances to take measures to prevent users from encountering or sharing child sexual abuse material (CSAM) [web].
[5] Ofcom (2025). DStorage's compliance assurances to take measures to prevent users from encountering or sharing child sexual abuse material (CSAM) [web].
[6] Ofcom (2026). Enforcement programme into measures being taken by file-sharing and file-storage services to prevent users from encountering or sharing child sexual abuse material (CSAM) [web]. See update on September 2026.
[7] IWF (2026). Separating fact from fiction on the technology used to detect child sexual abuse [blog].
[8] Ofcom (2026). Enforcement programme into measures being taken by file-sharing and file-storage services to prevent users from encountering or sharing child sexual abuse material (CSAM) [web]. See update on Oct 2025.
[9] Ofcom (2026). Investigation into the provider of Im.ge and its compliance with duties to protect its users from illegal content [web].

3.2.6. In terms of protecting children from accessing pornographic content, Ofcom's 2026 Use of Age Assurance Report states that 64 of the most popular pornographic services have deployed age checks as of June 2026.[10] The report also indicates that age assurance is presenting barriers for children trying to access pornographic content with nearly half of the pornography services visited by children had deployed age assurance (46%).[11] However, the report also notes that some children are moving towards services that do not require age checks.[12] Despite progress being slower than imagined, the rollout of age assurance is an important and promising signal to ensure children are not exposed to age-inappropriate content.

3.2.7. These developments demonstrate that a needed regulatory floor for tackling illegal content has been established and is progressing. Whilst developments have been slow, it does not detract from the fact that for the first time services are bound to introduce foundational safety measures

3.3. **Has the OSA been effective in protecting groups disproportionately affected by harms within its scope, including women and girls, and those vulnerable to exploitation?**

3.3.1. Women and girls continue to be disproportionately harmed online. Between January 2024 and December 2025, 76% of child sexual abuse imagery assessed by the IWF depicted girls.[13] IWF analysts also encounter content depicting violent sexualisation, misogynistic framing, degrading scenarios. This includes dedicated websites posting voyeuristic and non-consensual material. The content is often posted under the banner of "exposing" the victim as outlined by an IWF analyst[14]:

"Some online indecent imagery depicting older teenage girls and young women is disturbingly humiliating and framed by misogynistic language. We encountered a web user who described the posting and sharing of indecent imagery - including that of confirmed child victims - as "trading and exposing whores." Another user posted the nude image of a female with the text "your body is now the public property of the web." A strong sense of the commodification and ownership of women's and girls' bodies is evident in certain online spaces."

3.3.2. Regarding concrete measures to tackle VAWG, Ofcom issued Guidance in November 2025 on how service can address the content and activity which disproportionately affects women and girls.[15] Whilst the Guidance has been in place for over nine months it is unclear what the impact has been. In May 2026 Ofcom introduced a Code-requirement for in-scope services to implement hash-matching for detecting intimate

[10] Ofcom (2026). Report on the use of age assurance [pdf]. p. 22.
[11] Ibid. p. 29.
[12] Ibid. p. 28.
[13] IWF (2026). Internet Watch Foundation Annual Report 2025 - Violence Against Women and Girls [web].
[14] Ibid.
[15] Ofcom (2025). A Safer Life Online for Women and Girls - Practical Guidance for Tech Companies [pdf].

image abuse.[16] On the 9 September 2026, Ofcom announced it will be opening an enforcement programme to monitor the spread of non-consensual intimate image (NCII) abuse.[17] Whilst an enforcement programme for NCII is urgently needed the speed of regulation around safety of women and girls online has been particularly slow. We await Ofcom's May 2027 report which we hope will provide further clarity on the impact the regime has had on women and girls' safety online. [18]

3.3.3. As time has progressed the UK's armoury of levers has also expanded in efforts to keep up with the growing complexity and evolving nature of these harms. This means that assessment of the OSA, in tackling violence against women and girls, should also consider the Crime and Policing Act 2026 and the 2025 Violence Against Women and Girls strategy.[19] The introduction of the Crime and Policing Act has strengthened the response to NCII by creating a statutory NCII Register and requiring content to be taken down within 48 hours of reporting. The Starmer Government's 2025 Violence Against Women and Girls strategy set out how the former Government would meet their manifesto pledge to halve violence against women and girls over the next decade, and included commitments for device level protections on children's phones to protect them against unsolicited nude imagery.[20] We are pleased with the Government's recommitment to on-device nudity detection and welcome their decision to bring forward legislation and intervene where it matters most.[21]

3.3.4. AI tools can amplify harms to women and girls by enabling the generation of sexualised depictions at scale which can lead to mass circulation and revictimisation for women and girls. We welcomed the Crime and Policing Act establishing concrete steps to ban nudification apps as a product. However, the ban has yet to be brought into force. Additionally, this is expected to apply only to apps "designed" specifically to create non-consensual intimate imagery. This means general-purpose AI systems will likely remain outside the scope of the ban.

3.3.5. Importantly, regulation of AI is largely missing from the OSA. AI-generated child sexual abuse material represents a significant and evolving risk, as advances in technology make it easier to produce realistic and harmful content at scale. Such imagery can contribute to the ongoing exploitation of children, cause lasting harm to victims, and place increasing pressure on safeguarding, legal and regulatory systems. Imagery can be found on both the clear web and dark web.

---

[16] Ofcom (2026). Detecting intimate image abuse - Online Safety – Additional Safety Measures [pdf].
[17] Ofcom (2026). Ofcom to crack down on spread of illegal intimate images and deepfakes, boosting protections for women and girls online [news].
[18] Ofcom (2026). Ofcom's Plan of Work 2026/27 - Making communications work for everyone [pdf]. p. 17.
[19] Home Office (2026). Freedom from violence and abuse: a cross-government strategy to build a safer society for women and girls [web].
[20] Ibid.
[21] Hansard HC Debate (8 Sept 2026). Online Safety. Vol. 790, col. 917 – 918 [web].

3.3.6. Whilst any AI-generated content shared by users on a user-to-user service would be regulated in the same way as content generated by humans, chatbots are not subject to regulation if they:

- Only allow people to interact with the chatbot itself and no other users (i.e. they are not user-to-user services).
- Do not search multiple websites or databases when giving responses to users (i.e. are not search services).
- Cannot generate pornographic content.

Whether chatbots fall within one or more of the above categories depends on how they work. In instances where some AI chatbots are in scope of the OSA it does not mean that all content they generate will be regulated.

3.3.7. The Government must ensure that the regulatory framework for AI requires companies to embed safety by design, mitigate harm, and prevent the creation of AI-generated CSAM and NCII. Additionally, chatbots should be required to signpost users to support services where conversations involve references to child sexual abuse. Finally, interventions must be developed and rolled out in consultation with child-development experts to ensure that children and victims remain at the heart of the response. Please see section 3.6 for further views on safety by design.

3.4. **Have the OSA's provisions been effective in driving services to a) identify relevant risks, b) take proportionate action that adequately mitigates those risks, and c) make meaningful changes to their systems, processes and design features?**

3.4.1. Hash-matching was introduced under the first iterations of the Illegal Harms Code of Practice for in-scope services to detect and remove CSAM. As we mention in section 3.2, hash-matching is a foundational part of detecting known CSAM. Introducing hash-matching as a code measure means more services, particularly those at high-risk, are preventing the spread of images of child sexual abuse.

3.4.2. It is also positive that part 3 and part 5 services are required to use highly effective age assurance to ensure children are not able to access pornographic of age-inappropriate content, as we refer to in section 3.2. This is particularly important in preventing children from being exposed to extreme pornography which can increase the risk of normalising dangerous and harmful sexual behaviour in children, including image-based sexual abuse, coercive control, stalking, and physical assault. [22, 23, 24]

[22] Children's Commissioner (2024). "I've seen horrible things": children's experiences of the online world [pdf].
[23] CEASE UK (2025). Written evidence from CEASE UK [MIS0041] [pdf].
[24] Nation.Cymru (2025). Teenager jailed for sexually abusing 37 girls online [news].

3.4.3. However, the technical feasibility condition in Schedule 4 of the Online Safety Act has presented sizeable barriers for Ofcom to meet the intended ambitions of the Act. At present technical feasibility seemingly provides services with a get-out clause and has allowed them to circumvent their safeguarding duties. It is also difficult to incentive services to be proactive in their safeguarding duties since they are in 'safe harbour' by complying with code measures. This means that despite not meeting the ambition of the OSA, services are currently considered to have fulfilled their safety duties.

3.4.4. The challenge with technical feasibility is acutely felt when it comes to end-to-end encrypted (E2EE) services. The ambitions of the Online Safety Act cannot be fully felt while there remains a lack of ambition in tackling harms for E2EE services. E2EE can be abused for a wide range of serious crimes, including child sexual exploitation and abuse.[25] It has also been identified by Ofcom as a risk factor for CSAM detection.[26]

3.4.5. Publicly available evidence on the scale and severity of harm in encrypted environments is currently limited. This reflects the challenges of gathering data in encrypted environments and the limited legislative duties on services to proactively detect CSAM. The IWF is working to remedy this evidence gap by publishing an upcoming report evidencing the harms encountered by Analysts in public-facing parts of 'encrypted' services. We will be happy to submit the report for the Committee's consideration when it is available.

3.4.6. Despite this, we are aware that E2EE spaces are being used to sell and purchase CSAM. The IWF is not able to access end-to-end encrypted chats and therefore cannot comment on what occurs inside those chats. However, there is sufficient evidence in the public versions of these forums to indicate that CSAM is being shared and sold on E2EE services. We have submitted a sample of this evidence to Ofcom and will provide further evidence in our upcoming report.

3.4.7. Investigative work by law enforcement and research from child protection groups provides further sense of the scale of the harm. For example, a 2020 study by the CyberPeace Foundation found more than 100 instances of CSAM in 29 randomly selected adult pornography WhatsApp groups, which are end-to-end encrypted.[27] In 2026 Protect Children ran an anonymous self-report survey of adults searching for CSAM on the dark web.[28] The survey found: (1)12% of respondents reported using E2EE messaging services to access CSAM; (2) 20% of the respondents avoided using platform

[25] NCA (2024). European police chiefs call for end-to-end encryption roll out to include public protection measures [news].
[26] Ofcom (2026). Protecting people from illegal harms online: Register of Risks [pdf]. See 2B.67 – 2B.69.
[27] CyberPeace Foundation (2020). End (-to-end Encrypted) Child Sexual Abuse Material [pdf]. p. 3.
[28] Protect Children (2026). CSAM Perpetrator Research Report: Findings from a Survey of CSAM Perpetrators on Digital Platform Use and Design [pdf].

without E2EE; (3) and E2EE messaging services and tools were used by respondents to store CSAM.[29]

3.4.8. There is a lack of clarity on how Ofcom determines technical feasibility. Without clarity on the technical feasibility threshold, sizeable barriers remain for introducing safeguards in E2EE services. As a start, Government must clarify how technical feasibility will be judged to ensure that it is not used by platforms as a get-out clause to evade compliance.

3.4.9. Ofcom must then provide clear guidance on how it will assess when it is technically feasible for a service to implement measures and when it is not. It should provide case studies on the assessment of technical feasibility for particular features and functionalities and regularly update its guidance to reflect emerging technologies.

3.4.10. In IWF's response to Ofcom's Additional Safety Measures consultation, we raised that Ofcom should regularly review technological developments and update its Codes of Practice when safety measures become technically feasible. This includes preventing services from 'rolling back' on features in order to avoid implementing measures when they are considered technically feasible.[30] We also supported the Online Safety Network's (formerly known as the Online Safety Act Network) call for Ofcom to clarify the distinction between technical infeasibility and cost.[31]

3.4.11. In the Technology Notice Guidance, Ofcom noted that it can require services to use upload prevention, often known as 'client-side scanning', if necessary and proportionate to do. Upload prevention is a pre-encryption check that takes place on an image or video before content is shared.[32] However, Ofcom also noted that technical feasibility will remain a consideration before the decision is taken to issue a Technology Notice:

> *"we are satisfied that the Act provides us with a broad power to require the providers of regulated services to use accredited technology, including to prevent users encountering content (and therefore before that content is communicated by means of the internet service). We therefore disagree with the arguments that Ofcom does not have the power to require the use or development/sourcing of such technology, or that it could never be necessary and proportionate for Ofcom to require this. However, whether it is necessary and proportionate will depend on the specific circumstances, and we have not taken (nor do we consider that it would be appropriate to take) a view on whether technology currently exists that could be used on content before it is uploaded without unduly interfering with users' fundamental rights."* [33]

[29] Ibid. p. 19 – 24.
[30] Internet Watch Foundation (2025). Response to Ofcom's Additional Safety Measures Consultation [pdf].
[31] Ibid.
[32] Ofcom (2026). Statement: Technology Notices Guidance [pdf]. p. 29.
[33] Ibid. p. 29 - 30.

3.4.12. However, upload prevention or 'client-side scanning' is a technically feasible method for detecting known CSAM in E2EE environments which does not unduly interfere with other fundamental rights. The IWF's 2025 upload-prevention explainer outlines a privacy-preserving and readily deployable method for detecting known CSAM in E2EE environments.[34] The paper also covers how E2EE services such as WhatsApp already use this method to check messages for malware or to fetch a URL to create 'rich preview links.' It is also important to note that a victim or survivor has the fundamental right to privacy and preventing the recirculation of images of their sexual abuse.

3.4.13. Platforms operating in encrypted environments should not be exempt from foundational detection duties in the Online Safety Act. As a starting point, E2EE services must be mandated to detect and block CSAM before it can be encrypted. Pre-encryption checks, including upload prevention, provide a privacy-preserving way to detect images and videos of child sexual abuse.

3.4.14. The duty to proactively detect content is limited to that which is considered public under the Online Safety Act. [35] In December 2024 Ofcom issued guidance, in the form of case studies, illustrating when content is likely to be considered publicly communicated and when it is likely to remain private.[36] Notably, the guidance indicates that content shared within end-to-end encrypted group chats may, in certain circumstances, be regarded as public communication where the group contains a 'very large number of other users'. In such cases, the content could fall within the scope of proactive detection duties despite being shared via an E2EE service.[37] In Section 121 of the OSA, Ofcom is granted the powers to require services to use accredited technology to identify, take down, and prevent the encounter of child sexual exploitation and abuse content. This duty applies regardless of whether it is content communicated publicly or privately. The section also states that if Ofcom considers it necessary and proportionate, they may give a notice to a service provider to use its "best endeavours to develop or source technology for use on or in relation to the service or part of the service."[38] This further indicates that end-to-end encrypted content falls within the scope of proactive detection duties. It is crucial that Ofcom makes the most of its power under Section 121 of the Online Safety Act to compel companies to use their best endeavours to prevent images and videos of child sexual abuse from circulating in E2EE environments.

3.4.15. In summary, while the Online Safety Act and Ofcom's Codes of Practice have introduced important safeguards, including hash-matching and age assurance, their effectiveness will remain undermined if the technical feasibility condition is allowed to operate as a

[34]IWF (2025). Preventing the upload of child sexual abuse material (CSAM) in E2EE environments [pdf].
[35] See Section 232 of the Online Safety Act.
[36] Ofcom (2024). Protecting people from illegal harms online: Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act [pdf].
[37] Ibid. See case study 5.
[38] See section 121 2 (b) of the Online Safety Act.

barrier to meaningful action. This is particularly acute in E2EE environments where evidence indicates that CSAM is shared and sold yet services can avoid their foundational detection duties. Government and Ofcom must therefore provide clearer guidance on technical feasibility, keep pace with emerging technologies, and ensure that privacy-preserving measures such as upload prevention are used where necessary and proportionate to detect and block CSAM before it can be encrypted or recirculated.

3.5. **Has the OSA impacted users' ability to report illegal content or content harmful to children, make complaints and receive an appropriate and timely response, and to what extent?**

3.5.1. The IWF cannot speak to the impact the OSA has had on users being able to report content directly to services as this information is not available to us. In this section, we discuss how children are using our reporting portal. Reports of CSAM to the IWF have continued to increase, but it is unclear whether the OSA has directly impacted this.

3.5.2. Report Remove is a reporting service provided by the IWF and Childline that allows children under 18 to report and remove sexual images or videos of themselves from the internet. Children using the Report Remove tool can submit up to 50 images or videos in a single report and may make multiple reports.

3.5.3. In 2025, Report Remove received 1,894 reports, representing a 66% increase compared with 2024. The service took action on 1,175 reports in 2025, an additional 533 reports compared with 2024. Actioned reports consisted of 2,963 individual criminal images and 509 criminal videos. Boys aged 14 to 17 were the primary users of the service. They accounted for 98% of sexually coerced extortion reports.[39]

3.5.4. Boys are often lured into what they believe to be consensual exchanges of sexual images with peers, but are in fact being groomed into sharing imagery without their consent. Sexually coerced extortion is evidenced in Report Remove reports through material such as chat logs demonstrating coercive behaviour, or collages created by offenders in which images are combined and overlaid with threatening or intimidating text.[40]

3.6. **What unintended consequences, if any, have arisen from the Act or its implementation, including for freedom of expression, privacy and accessibility?**

3.6.1. An unintended consequence of the Act is Ofcom's cautious interpretation of the powers it has been given, particularly in relation to technical feasibility, safety by design and safe harbour. The Online Safety Network's (formerly known as the Online Safety Act Network) 10-point plan, supported by the IWF, outlines the challenges arising from Ofcom's approach and how these can be addressed.[41]

[39] IWF (2026). Internet Watch Foundation Annual Report 2025 - Analysis of Report Remove [web].
[40] Ibid.
[41] Online Safety Network (2026). STRENGTHENING THE ONLINE SAFETY ACT: A TEN-POINT PLAN FOR GOVERNMENT [pdf].

3.6.2. However, it is within Government's powers to amend the OSA, through targeted amendments, to align Parliamentary intent with Ofcom's approach to implementation. We are particularly concerned by the unintended consequences from the following aspects of the Online Safety Act: technical feasibility (discussed in response to section 3.4), safety by design, and safe harbour.

3.6.3. Safety by design is a central principle for digital regulation and is set out in the introductory clause of the Online Safety Act. While there is broad agreement on what safety by design means, there is less certainty about what it specifically requires and how it should operate in practice. As Professor Lorna Woods has outlined, an introductory clause sets out the purpose of legislation.[42] This reinforces what the Government minister responsible for the then Online Safety Bill through the House of Lords stated:

> *"the new introductory Clause 1 makes this explicit as an overarching objective of the Bill. The introductory clause does not introduce any new concepts; it is an accurate summary of the key provisions and objectives of the Bill and, to that end, the framework and introductory statement are entirely compatible."*[43]

3.6.4. Safety by design should therefore be understood as a whole-system approach that must be considered from product design through to the governance of the service. Many aspects of this require a preventative and proactive response. However, Ofcom's current implementation of the OSA focuses on downstream measures that target harms after they have occurred. To remedy this contract in approach, a statutory definition of safety by design must be inserted into the OSA to make clear to Ofcom and regulated services what Parliament intended. Secondary legislation should also be laid to require Ofcom to produce a cross-cutting Safety by Design Code of Practice.[44] This would sit beneath the existing content-based codes and operationalise the intention of the OSA.

3.6.5. The safe harbour provision in section 49(1) of the Online Safety Act removes the incentive for companies to exceed Code requirements and, in turn, limits innovative safety measures. It fails to raise the bar for ambitious safeguarding measures and innovation across the sector which in the case of E2EE has detrimental impacts. We support the Online Safety Network's calling for the removal of the safe harbour provision from the OSA.[45]

---

[42] Online Safety Network (2026). SAFETY BY DESIGN [pdf]. p. 2.
[43] Ibid.
[44] Online Safety Network et al. (2026). Safety by Design Code of Practice [pdf].
[45] Online Safety Network (2026). STRENGTHENING THE ONLINE SAFETY ACT: A TEN-POINT PLAN FOR GOVERNMENT [pdf].

3.7. **Has Ofcom's interpretation and implementation of the OSA to date given appropriate effect to its provisions?**

3.7.1. Please see our response in section 3.6.

3.8. **What changes, if any, are needed to improve the effectiveness of Ofcom's a) illegal content and protection of children codes of practice, b) guidance on violence against women and girls, or c) wider regulatory approach?**

3.8.1. To improve the effectiveness of Ofcom's Illegal Content Codes of Practice and Protection of Children Codes of Practice. the following changes are required:

- Further clarity and guidance on the technical feasibility condition. Please see our response in section 3.4.

- The introduction of safeguards for end-to-end encrypted spaces. Please see our response in section 3.4.

- The incorporation of a safety-by-design definition in the Online Safety Act, coupled with the adoption of a Safety by Design Code of Practice. Please see our response in section 3.6.

- The removal of the safe harbour provision from the Online Safety Act. Please see our response in section 3.6 and 3.4.

3.8.2. These changes in turn will also wield positive impacts for tackling both violence against women and girls and supporting the wider regulatory approach for online safety.

3.9. **Where duties are in force, how effective and timely have Ofcom's supervision and enforcement been in driving improvements and securing compliance?**

3.9.1. N/A

3.10. **Are there any factors that may be limiting Ofcom's ability to carry out its duties under the OSA effectively? If so, what changes are needed?**

3.10.1. Please see our response in section 3.8.

3.11. **What specific changes, if any, are needed to the existing provisions in the OSA to improve their effectiveness?**

3.11.1. In response to the former Government's consultation *Growing up in the online world: a national consultation* ('Growing up online'), the IWF and eight other civil society organisations dedicated to tackling online CSEA provided a list of urgently needed interventions to provide life-altering outcomes for children's safety online. Submitted under the banner of the UK Alliance Tackling Online CSEA (UK ATOC), the interventions

were categorised into technical and legislative and provided a non-exhaustive list spotlighting measures that were a collective priority for all of us. We would encourage the Committee to consider UK ATOC's recommendations submitted as part of its work.[46]

3.11.2. Many of the UK ATOC recommendations have already been discussed in our response including our concerns with E2EE (see section 3.4), technical feasibility condition (see section 3.4), safety by design and safe harbour (see section 3.6).

3.11.3. The UK ATOC consultation response also outlines the need for greater collaboration between UK regulators to improve the effective of the OSA. A coordinated regulatory approach is essential to ensure that emerging harms from new products and services do not fall between institutional responsibilities. This can begin by placing a duty on Ofcom to cooperate with domestic regulators in the way it must with international regulators. Additionally, the Digital Regulation Cooperation Forum (DRCF) should be placed on statutory footing.[47]

3.11.4. In the UK ATOC response we also noted that there should be responsibility to ensure that all AI chatbots are adequately regulated under the OSA. Through the Crime and Policing Act, the Secretary of State has been granted powers to amend the OSA to bring chatbots within the scope of the Act's illegal-content duties.[48] This means that legal liability for chatbot companies remains unclear, with coverage partial and uneven. There is also little clarity on when the Secretary of State intends to exercise these powers or when the Government will publish a timetable for implementing its proposed ban on sexualised chatbots for under-18s.

3.11.5. To ensure that AI chatbot services are fully within the scope of regulatory obligation, further legislative amendments are needed. These amendments should consider risk assessments and transparency notices for AI chatbots, legal requirements for robust product testing, penalties for failing to mitigate and manage risks, and signposting to provide victim support or behavioural changes.[49]

3.11.6. We also support the Online Safety Network's to future-proof the Online Safety Act by introducing an overarching duty of care. This will require a more systemic approach to risk assessment and mitigation by regulated services. The duty of care should include emerging harms arising from new products and services.[50 & 51]

---

[46] UK ATOC (2026). Growing up in the online world: Collective recommendations for tackling the risks of online child sexual abuse and exploitation [pdf].
[47] Ibid. p. 12.
[48] Ibid. p. 9.
[49] Ibid.
[50] Ibid. p. 12.
[51] Online Safety Network (2026). STRENGTHENING THE ONLINE SAFETY ACT: A TEN-POINT PLAN FOR GOVERNMENT [pdf].

3.12. **Beyond amending the OSA, what specific action should the Government, Ofcom, regulated services or Parliament take to address any shortcomings in the online safety regime?**

3.12.1. With the Department for Science Innovation and Tech (DSIT) being divided up, there is an opportunity to start afresh and reset relationships to enable more meaningful engagement.

3.12.2. Child-safety groups have previously received significantly less access to the Government department holding the brief for the OSA, compared to technology companies. As noted in the 2026 Guardian article, "technology companies and their lobbyists attended at least 639 meetings with ministers compared with just 75 meetings attended by the organisations and campaigners fighting for greater protections for children online, such as the NSPCC."[52] Meaningful and more frequent engagement with civil society will be an important starting point for counterbalancing this dominant tech-sector lobbying.

3.12.3. We are also concerned that under the current Government, the online safety brief is not being given the priority it deserves. The brief for the Secretary of State for the Department for Digital, Culture, Media and Sport (DCMS) is large and significantly varied. We are concerned that this may put online safety at risk of becoming lost among other competing priorities. The complexity and scale of the CSEA risks online continues to increase in 2025 the IWF actioned 311, 610 reports which confirmed to contain or lead to CSAM, we saw a 66% increase in Report Remove submissions, and a 260-fold increase in AI generated CSA videos.[53] It is imperative that online safety is prioritised to meaningfully deliver on the ambitions of the OSA.

3.13. **How well can the existing online safety framework respond to emerging harms and technologies? What changes, within the existing framework of the Act, are needed to ensure that it remains fit for the future, and should these be made within the existing framework or through further primary legislation?**

3.13.1. Please see our response in section 3.11.

3.14. **What impact could the recent and proposed additions to the UK's online safety framework, including the Government's proposals to restrict access to social media for under 16s, have on the OSA's implementation and effectiveness?**

3.14.1. The IWF, alongside with eight other leading civil society organisations, provided our views on the impact of an under-16 social media ban followed by our suggested recommendations in response to the *Growing up in the online world: a national consultation*. As we outline in section 3.11, these interventions were jointly developed

[52] The Guardian (2026). Tech companies' access to UK ministers dwarfs that of child safety groups [news].
[53] IWF (2026). Internet Watch Foundation Annual Report 2025 – Executive Summary [web].

and submitted under the banner of the UK Alliance Tackling Online CSEA (UK ATOC) which provides a forum for collaboration on shared policy priorities.

3.14.2. In our view, an under-16 ban *may* contribute towards ensuring children's safety online, but it should not be viewed as a standalone solution to tackling online CSEA. CSEA is a complex threat area where risks cannot be pinpointed to a single factor such as harmful design choices. Equally, the risk of harm does not stop at age 16 and in fact children aged 14 to 17 are among the primary users of Report Remove.[54]

3.14.3. With the introduction of the ban, and the relegating of online safety within a wide and disparate range of topics under the new Government (see our response to section 3.12), we are concerned that children's safety online may be viewed by Government as a 'one-and-done' solution.

3.14.4. To turn the tide against online harms, the Government must introduce a package of interventions that target different stages of the CSEA pathway, from prevention through to tackling revictimisation as we outline in our 'Growing up online' consultation response. In our consultation submission we also provided a table mapping the likely contribution that each of our proposed interventions would have on reducing key online CSEA threats. UK ATOC updated the table in response to the Government announcement of a ban.[55] We encourage the Committee to consider both UK ATOC's submission and our updated interventions tables as part of its work.

3.14.5. Finally, we are concerned that enforcement of a social media ban may detract in the short term from Ofcom's ability to deliver on its existing duties under the OSA. It is important Government ensures Ofcom has the needed resourcing to deliver on both its existing responsibilities under the Online Safety Act as well as any new responsibilities, including a social media ban.

[54] IWF (2026). Internet Watch Foundation Annual Report 2025 - Analysis of Report Remove [web].
[55] UK ATOC (2026). UK Alliance Tackling Online CSEA (UK ATOC) response to the UK social media ban [statement].