Consultation response form

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	Confidential? – No No views as to this question.
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.	Confidential? – No No views as to this question.
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?	Confidential? – No No comments as to this question.
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.	Confidential? – No No views as to this question.

Question	Your response
Question 5: Do you have any comments on our draft Technology Notice Guidance?	Confidential? – No Our response raises the following key points: • The differential treatment of developed/sourced technology and accredited technology • The risks of subverting end-to-end encryption • Potential conflicts of laws considerations • Compelled speech considerations • The risks of mission creep • The lack of review mechanisms • The absence of a role for the Information Commissioner. **A 3.6/3.7 Distinctions between developed/sourced technology and accredited technology** First, we are concerned by the differential treatment of developed/sourced technology and accredited technology, which both would carry similar risks to fundamental rights and freedoms. A3.7(f) of the draft Guidance notes that when a Technology Notice requires a service provider to **develop or source technology**, Ofcom is not required to consider the factors set out in A3.6 (considerations of freedom of expression, privacy, and availability of journalistic content/sources and less intrusive measures). We appreciate that this distinction arises due to s. 124(4)(b) of the Online Safety Act (OSA) 2023. While the Guidance notes that Ofcom expects that it would consider the A3.6 factors, there are at least two arguments in favour of Ofcom adopting a stronger position on this point (even if not required by s. 124 to do so): a practical reason and a related legal reason. In terms of the former, if ultimately the use of any such developed or sourced technology would clearly not be possible due to the risk of impact on e.g. freedom of expression and privacy, then Ofcom would have superfluously required the use of resources by the service provider(s) in its development or sourcing of technology. This may itself interfere with internationally recognised rights (such as the right to conduct a business, or related rights such as the right to property and freedom of contract). In terms of the latter, if, in the end, service providers choose to utilise any sourced or developed technology

Question	Your response
	(even if not legally compelled to do so by Ofcom), and it does prove to interfere significantly with the human rights of individuals (e.g. due to interferences with privacy), Ofcom's initial involvement could expose it to liability for breach of the Human Rights Act 1998 (s. 6(1)). A Technology Notice that requires the service provider to develop or source technology carries with it the likely implication that the technology will then be used for the purpose of monitoring public or private communications. Thus, the impact on fundamental rights must also be considered before issuing Technology Notices to source/develop technology. On this second legal point, we also suggest that the Guidance clarify that there is no obligation on the provider to *use* the sourced technology for any of the acts specified in e.g. s121(2)(a) or s. 121(3)(a). Second, we find the guidance lacks sufficient detail on the practical consequences of a notice to develop or source technology for use on or in relation to the service (or part of the service). For example, the section concerning the content of warning notices (A6.5(b)) suggests that Ofcom would not 'require the service provider to allow the technology it has developed or sourced to be used by another service provider in a Notice' but this is not categorically ruled out and there is no discussion of the intellectual property implications involved. Similarly, the section concerning 'further notices' (A7.11-A7.14) raises a range of questions relating to when a further notice will be given in relation to any 'developed or sourced' technology and what could be required thereby. We would expect that this section would address in greater detail issues that may not be apparent from the legislation. For example, it is not clear what process would be followed on some points where developed or sourced technology could become subject to a subsequent *use* notice as accredited technology, or otherwise (para 2.35 of the consultation document, for example, alludes to a broad interpretation of an Ofcom power to 'require the use of technology for the purposes set out in section 121'). On one reading, safeguards like the skilled person's report could be discarded in the case of such a further notice (A7.13 of the Guidance, and s. 126(9) OSA 2023). We suggest that these implications –

Question	Your response
	after there is service provider compliance relating to a notice to develop or source technology – require much greater attention and explanation in the Guidance. **A3.8 Other matters Ofcom are likely to consider** A3.8 sets out other matters that Ofcom are *likely to consider* before issuing a Technology Notice. These considerations are essential for each Technology Notice and require further additions, including (1) further guidance on technical feasibility and encryption and (2) the addition of consideration regarding potential conflicts of laws. First, A3.8(a) notes that **technical feasibility** should take into account the way the service is configured. The guidance should be clear that if the service is configured with end-to-end encryption, a Technology Notice will not require such encryption to be removed or weakened. This would make explicit what the government was said to have intended with s. 121 OSA 2023. Lord Parkinson (Parliamentary Under Secretary of State in the Department of Culture Media and Sport) provided assurances to members of the House of Lords at the time of the passing of the Bill that 'there is no intention by the Government to weaken the encryption technology used by platforms'. (Hansard, HL Deb 6 September 2023, vol 832, col 457.) Related to this point, we are especially concerned that the draft guidance does not explain what is meant by technical feasibility, how that will be determined and the types of considerations that will be taken into account in this assessment. Technical feasibility is not defined in the Act, even though it was stated as a criterion by government in its assurances related to the potential impact of s. 121. As a result, it is incumbent on Ofcom to provide further elaboration on this concept in the draft Guidance. We are particularly concerned that the consultation 'does not take a view on … [t]he extent to which there is technology available that could be used to identify or prevent users encountering terrorism or CSEA content in any particular deployment scenarios, **for example end-to-end encrypted environments**." (para 2.34 of the Consultation document). This is the elephant in the room, as it is

Question	Your response
	not clear what is permitted by the OSA 2023 in this context. On one view, Ofcom cannot require a solution (even if 'technically feasible') that would have the effect of *circumventing* encryption (through, for example, the utilisation of client scanning technologies) as this could 'weaken encryption'. On another view, circumvention of encryption could be required through Technology Notices, if the underlying encryption would remain intact. Computer scientists warn of systemic risks in uses of technology that circumvent end-to-end encrypted communications and have called for rigorous *public* review and testing before any consideration is given to mandating its use. We are particularly concerned that such a review will not occur prior to the implementation of the Technology Notice regime, and this would appear to be an even greater risk where Ofcom relies on notices to 'develop or source technology where a Notice to use accredited technology is not an option.' (para A3.12 of the Guidance). Public review cannot occur if the public are unaware of how Ofcom intend to implement these powers with respect to end-to-end encrypted communications. Moreover, the lack of clarity as to the scope and possible effect of the s. 121 powers in the context of end-to-end encrypted communications will be a significant factor in any future legal consideration of these powers from a human rights perspective. A court that is called upon to consider potential interferences with e.g. the right to privacy, would have to consider the 'quality' of the law. The fact that one cannot state with any certainty what the implications of s. 121 are – which the Guidance does not shed any further light on – would contribute to an argument that the Notice regime does not meet the quality of law requirements of, for example, Article 8 of the European Convention (ECHR). [For more on these points, see: Scott and Ó Floinn, 'Technical backdoors and legal backdoors: regulating encryption in the UK' (2024) 35(3) King's Law Journal 441; Shurson, 'A European right to end-to-end encryption?' (2024) 55 Computer Law & Security Review; Keenan, 'State access to encrypted data in the United Kingdom:

Question	Your response
	The 'transparent' approach' (2019) 49 Common Law World Review 223. – all available by email] Second, a further consideration should be added to A3.8 on the potential for **conflicts of laws**. In addition to considerations A3.8(b) on size and capacity of the provider and A3.8(c) on financial cost to the provider, Ofcom should consider whether the provider may violate the laws of a third country in complying with a Technology Notice. This requirement would be consistent with similar considerations for technical capability notices under the Investigatory Powers Act (IPA) 2016. The IPA Code of Practice specifies that the Secretary of State, when giving a notice to an operator based in a third country, should consider 'any requirements or restrictions under the law of that country that may arise when the operator complies' with the notice. (IPA Interception of Communications Code of Practice 2022, 8.13) Relatedly, A2.23 correctly notes that requirements in a Technology Notice will only be imposed in relation to the operation of a service in the UK or as it affects UK users of the service. This is an important limitation that is needed to avoid conflicts of laws with third countries. While it is difficult to consider the impact of Technology Notices when no accredited or sources technologies yet exist, computer scientists have warned that it may be impossible for these technologies to be used to target users within one country, given the global nature of these providers and their services. If the technologies required by notices are not able to target only UK users, then the attendant extraterritoriality creates the potential for conflicts of liabilities on service providers. Ofcom must consider this potential for conflicts to arise, and the implications which follow therefrom. The impact on the providers may be significant – exposing them to legal and financial risk – which may result in the withdrawal of necessary services from the UK market. **Additional guidance that should be included** **Compelled Speech**

Question	Your response
	With regards to the guidance at A3.8d on **other rights** protected by the ECHR, Ofcom should consider that requiring the development of new digital technologies under penalty of law is a form of compelled speech. Code is a recognised mode of expression protected by copyright, and compelling the development of code is an interference with the rights of service providers that would have to be justified. Whilst this issue should be considered within an overall proportionality assessment, it is a dimension so far overlooked. It will likely be of greater import to individuals and organisations based in other jurisdictions yet subject to Ofcom's jurisdiction in respect of UK users or services. With regards to the guidance at A3.8c on **financial cost**, Ofcom should not only consider the proportionality of costs in relation to an individual service's financial position but also in relation to the market in services. An intervention by Ofcom is not merely a regulatory measure but a public event that will differentially impact some services over others. There is a real risk that the market in UK digital services is negatively impacted in terms of investment and innovation by the bespoke requirements of the OSA, which will drive investment into alternative jurisdictions. **Mission Creep** Ofcom's guidance at A3.4-A3.6 and A6.12 makes clear that in each case where a decision on whether a Technology Notice is considered, the assessment will be highly fact-specific and that two service providers which raise similar grounds for concern may be assessed differently in relation to necessity and proportionality (as stated at A3.4). Ofcom provides no indication as to how the relevant factors will be weighed, simply stating that it will have 'regard to the available evidence' (A4.10) in making initial assessments and 'all relevant evidence' (A6.11) in making a final decision on whether to issue a TN. While we recognise that an open-ended approach to the list of considerations that Ofcom will factor into each decision serves to allow recognition of important differences between services, we are concerned that it also allows justifications for Technology Notices to be found contingently in response to external pressures.

Question	Your response
	We suggest that the considerations at A3.6 regarding privacy, data protection, freedom of expression and journalistic content, alongside the availability of less intrusive measures, must be **prioritised** in making a proportionality assessment. We make this point because we are concerned that the reality of making risk-based assessments on matters concerning politically sensitive issues like terrorism and combatting CSEA material (and the public relations strategies employed by private communication service providers operating in a competitive market) means that Ofcom will be in the position of either applying a blanket risk-averse approach to implementation of scanning technologies, or justifying differential decision-making between factually similar cases. This is because a decision to impose a notice on one provider in relation to UK users but not a similar service will be read, in effect, as an intervention in the market (as noted above). In these circumstances there is a risk of 'mission creep' in respect of Technology Notices. The pressure to apply measures equally may lead to an expansive approach to the implementation of scanning technologies across services provided to UK users. We also note that the notification process, including the information-gathering stage and the Warning Notice stage (A6.4-6.5), is intended to encourage services to proactively engage with Ofcom's concerns (A6.9), although other reasons may ultimately be given for issuing a Technology Notice following representations (A6.16). Yet without robust red-lines on the necessity of implementing Technology Notices – for instance, a principle that a Notice is a *last resort* to be used where no other less intrusive measures have worked in relation to a service that is otherwise not in compliance with its lawful duties under the OSA – we are concerned that Ofcom will come under political and public pressure to justify or amend its decisions in individual cases. Public perception of mission creep would be to the detriment of the overall aims of the Act and to the market in digital services in the UK, while chilling freedom of expression. It may also leave Ofcom open to litigation, where narrow factual differentiations will be referred to courts, which may take different views to Ofcom's assessments.

Question	Your response
	These concerns are particularly acute where, as noted above, the measures required by a Technology Notice impact upon the protection of user privacy and freedom of expression provided by encrypted private messaging functions. **Review and appeal mechanisms** Relatedly to the problem of mission creep and the associated litigation risk, we note that unlike the comparable process that allows the Secretary of State to issue a Technical Capability Notice under the IPA 2016, there is no provision for a service provider to seek review of a notice prior to initiating an appeal to the Upper Tribunal under s.168 OSA. While the OSA does not provide for such a review mechanism in the way that the IPA does, there is no reason that Ofcom could not internally implement such a review mechanism in order to minimise litigation risks. This is particularly important considering that at A6.16, Ofcom reserves the right to make Technology Notices for reasons distinct to reasons canvassed at the prior information-gathering and Warning Notice stages. There is a potential gap in the mechanisms provided for representations (e.g. in s. 123 OSA) and consultations (e.g. in s. 126) within the legislative framework, and there should, as a result, be further provision made for internal review. Put simply, the reasons for enforceable notification decisions should always be reviewable without the risks of litigation and costs arising. **Information Commissioner consultation** We note that there is no requirement for Ofcom to consult with the Information Commissioner's Office (as currently constituted) in making assessments under A3.6. We suggest that incorporating the views of the ICO in relation to data protection and privacy would increase the legitimacy of such decisions. Similarly, there is no reason that Ofcom could not consult with other stakeholders than the target of the proposed Technology Notice, or with experts on privacy and human rights.

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