Technology Notices to deal with terrorism content and/or CSEA content

Annexes 6-8: Legal Framework, Impact Assessment & Glossary

Consultation

Published: 16 December 2024
Closing date for responses: 10 March 2025

Contents

Annex

A6. Legal framework: Ofcom's Technology Notice powers

A6.1 In Section 2, we have provided a high-level overview of Ofcom's powers under Chapter 5 of Part 7 of the Act. The purpose of this annex is to provide a more detailed overview of the statutory provisions relevant to Ofcom's Technology Notice functions.

A6.2 The overview in this annex should not be considered as an exhaustive summary of the law in this area. Readers are advised to read the Act for this purpose.

Who Ofcom can give a Technology Notice to

A6.3 Ofcom can only give a Technology Notice to the provider of:

a) a 'regulated user-to-user service', which means an internet service through which content that is generated, uploaded or shared by users may be encountered by other users of the service;[1]
b) a 'regulated search service', which means an internet service that is, or includes, a search engine;[2] or
c) a 'combined service', which is a regulated user-to-user service that includes a public search engine.[3]

A6.4 Such services will be 'regulated' if they have 'links with the United Kingdom'[4] and do not fall within Schedule 1 or Schedule 2 to the Act.[5] A service has links with the UK if it has a significant number of UK users or if UK users form one of the target markets (or the only target market).[6] A service will also be considered to have links to the UK if it is capable of being used in the UK by individuals, and there are reasonable grounds to believe that there is a material risk of significant harm to individuals in the UK presented by user-generated content present on the service or search content of the service.[7]

A6.5 We refer to these as 'Part 3 services' and providers of such services as 'Part 3 service providers' (or 'service providers') in this consultation.[8]

What Ofcom can require in a Technology Notice

A6.6 The Act provides Ofcom with the power,[9] if we consider it necessary and proportionate, to give a Technology Notice to a Part 3 service provider requiring it to:

[1] Section 3(1) of the Act.
[2] Section 3(4) of the Act.
[3] Section 4(7) of the Act.
[4] Section 4(2)(a) of the Act.
[5] Section 4(2)(b) of the Act.
[6] Section 4(5) of the Act.
[7] Section 4(6) of the Act.
[8] Regulated user-to-user and regulated search services are defined in the Act as 'Part 3 Services' because Part 3 of the Act imposes duties on providers of these services. We have adopted this definition throughout this consultation.
[9] Section 121(1) of the Act.

a) use accredited technology to deal with terrorism content and/or CSEA content (or 'relevant content'); or

b) use best endeavours to develop or source technology which meets minimum standards of accuracy to deal with CSEA content.

A6.7 Where we refer to 'accredited technology', we mean technology that has been accredited by Ofcom (or another person appointed by Ofcom) as meeting minimum standards of accuracy in the detection of relevant content.[10] The 'minimum standards of accuracy' are standards approved and published by the Secretary of State, following advice from Ofcom.[11]

A6.8 Subject to paragraph A6.9 below, a Notice requiring the use of **accredited technology** may require the providers of:

a) regulated user-to-user services to use that technology to identify and swiftly take down, or prevent individuals from encountering, terrorism content and/or CSEA content;[12] and

b) regulated search services to use that technology to identify search content of the service that is relevant content and swiftly take measures to secure that, so far as possible, search content no longer includes such content identified by the technology.[13]

A6.9 For regulated user-to-user services, we can require them to use accredited technology, or to develop or source technology, to address CSEA content communicated both privately and publicly by means of the service. However, a Notice requiring the use of accredited technology to address terrorism content can only require the use of that technology to address content communicated publicly by means of the service.[14]

A6.10 A requirement to use accredited technology may be complied with by use of the technology alone or by means of the technology together with the use of human moderators.[15]

A6.11 For a Notice relating to the **development or sourcing** of technology, Part 3 services may be required to use best endeavours to develop or source technology which meets minimum standards of accuracy and can be used:

a) in the case of regulated user-to-user services, to identify and swiftly take down, or prevent individuals encountering, CSEA content communicated publicly and privately;[16] and

---

[10] Section 125(12) of the Act.
[11] Section 125(13) of the Act.
[12] Section 121(2)(a) of the Act.
[13] Section 121(3)(a) of the Act.
[14] Section 232 of the Act specifies the following factors which we must, in particular, consider when deciding whether content is communicated 'publicly' or 'privately' for the purposes of a Technology Notice to deal with terrorism content: a) the number of individuals in the UK who are able to access the content by means of the service; b) any restrictions on who may access the content by means of the service; and c) the ease with which content may be forwarded to or shared with users of the service other than those who originally encounter it, or users of another internet service. See also Ofcom's Guidance on content communicated 'publicly' and 'privately'.
[15] Section 121(5) of the Act.
[16] Section 121(2)(b) of the Act.

b) in the case of regulated search services, to identify search content of the service that is CSEA content and swiftly take measures to secure that, so far as possible, search content no longer includes CSEA content identified by the technology.[17]

A6.12 A Notice may require a combined service to do any, or a combination, of the things described above in relation to the user-to-user part and/or search engine function of the service.[18]

A6.13 We may impose requirements in a Technology Notice only in relation to the design and operation of a Part 3 service in the UK, or as it affects UK users of the service.[19]

Additional requirements

A6.14 Where we issue a Technology Notice requiring the use of accredited technology, it is taken to require the service provider to make such changes to the design or operation of the service as are necessary for the accredited technology to be used effectively.[20]

A6.15 If a service provider is already using accredited technology in relation to the service, we may require that the service provider use the accredited technology more effectively and specify how that must be done.[21]

A6.16 A Technology Notice may also require the service provider to operate an effective complaints procedure, which:

a) in the case of a user-to-user service (or user-to-user part of a combined service), allows for UK users to challenge the provider for taking down content which they have generated, uploaded or shared on the service;[22]

b) in the case of a search service (or search engine of a combined service), allows for an interested person to challenge measures taken or in use by the service provider that result in content relating to that interested person no longer appearing in search results of the service.[23]

Steps and considerations for Ofcom before issuing a Technology Notice to a particular Part 3 service provider

A6.17 We have already provided an overview, from paragraph 2.25 of this consultation, regarding some of the steps and considerations before Ofcom can issue a Technology Notice to a particular Part 3 service provider. We do not repeat these in this Annex but have provided further detail on some of these below.

[17] Section 121(3)(b) of the Act.
[18] Section 121(4) of the Act.
[19] Section 125(10) of the Act.
[20] Section 125(5) of the Act. See also paragraph 598 of the Explanatory Notes to the Act, which explains that such changes must be proportionate.
[21] Section 125(2) of the Act.
[22] Section 125(3) of the Act.
[23] Section 125(4) of the Act. 'Interested person' means a person that is responsible for a website or database capable of being searched by the search engine, provided that: a) in the case of an individual, the individual is in the UK; b) in the case of an entity, the entity is incorporated or formed under the law of any part of the UK (section 227(7) of the Act).

Skilled person's report

A6.18 Before we may issue a Technology Notice, Ofcom is required to obtain a report from a skilled person, appointed by us, to assist us in deciding whether to give a Notice, and to advise about the requirements that might be imposed. A 'skilled person' means a person appearing to Ofcom to have the skills necessary to prepare a report about matters relevant to those purposes.[24]

Warning Notice

A6.19 We must give a Warning Notice to the service provider before we may issue a Technology Notice. Section 123 of the Act sets out the information that we must include in a Warning Notice depending on whether it relates to the use of accredited technology[25] or to the development or sourcing of technology.[26] In either case, a Warning Notice must provide the service provider with an opportunity to make representations to Ofcom on our intention to issue a Technology Notice.[27]

Ofcom must be satisfied that a Technology Notice is necessary and proportionate

A6.20 Section 124 of the Act set out the matters which we must particularly consider when deciding whether it is necessary and proportionate to issue a Technology Notice. These are:

a) the kind of service it is;

b) the functionalities of the service;[28]

c) the user base of the service;

d) in the case of a notice relating to a user-to-user service (or to the user-to-user part of a combined service), the prevalence of relevant content on the service, and the extent of its dissemination by means of the service;

e) in the case of a notice relating to a search service (or to the search engine of a combined service), the prevalence of search content of the service that is relevant content;

f) the level of risk of harm to individuals in the United Kingdom presented by relevant content, and the severity of that harm;[29]

g) the systems and processes used by the service which are designed to identify and remove relevant content;[30] and

h) the contents of the skilled person's report obtained.

[24] Sections 122 and 104(3), (4) and (6)(a) of the Act.
[25] Section 123(2) of the Act.
[26] Section 123(3) of the Act.
[27] Section 123(2)(f) and (g) and (3)(f) and (g) of the Act.
[28] 'Functionality' is defined in section 233 of the Act.
[29] See section 234 of the Act for the meaning of 'harm'.
[30] 'Systems and/or processes' refers to human or automated systems and/or processes, including technologies (section 236(1) of the Act).

A6.21 Where we are considering issuing a Notice requiring the use of **accredited technology**, we must also consider:

a) the extent to which the use of the specified technology would or might result in interference with users' right to freedom of expression within the law;[31] and

b) the level of risk of the use of the specified technology resulting in a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data).

A6.22 In the case of a notice relating to a user-to-user service (or to the user-to-user part of a combined service), the extent to which the use of the specified technology would or might:

a) have an adverse impact on the availability of journalistic content on the service,[32] or result in a breach of the confidentiality of journalistic sources; and
b) whether the use of any less intrusive measures than the specified technology would be likely to achieve a significant reduction in the amount of relevant content.

What information must Ofcom include in a Technology Notice

A6.23 The Act specifies information that must be included in a Technology Notice depending on whether the Notice relates to the use of accredited technology or to the development or sourcing of technology. We have provided further detail on some of the information we are required to provide below.

Timescales for compliance

A6.24 In the case of a Technology Notice to use **accredited technology**, we must specify:

a) a reasonable period for compliance with the Notice;[33] and

b) the period within which the requirements imposed by the Notice will have effect.[34] This may be for up to 36 months from the last day of the period for compliance (set out at a) above).[35]

A6.25 Where we issue a Technology Notice relating to the **development or sourcing of technology**, the Notice must specify a reasonable period within which each of the steps specified in the Notice must be taken.[36] We must take into account the size and capacity of the service provider, and the state of development of technology capable of achieving the

[31] 'Freedom of expression' means the freedom to receive and impart ideas, opinions or information (referred to in Article 10(1) of the European Convention on Human Rights) by means of speech, writing or images (section 236(1) of the Act).
[32] See section 19 of the Act for the meaning of 'journalistic content'.
[33] Section 125(6)(e) of the Act.
[34] Section 125(6)(f) of the Act.
[35] Section 125(7) of the Act.
[36] Section 125(8)(d) of the Act.

purpose for which the technology is to be developed or sourced, in deciding what period(s) to specify.[37]

Review of a Technology Notice

A6.26 We must carry out a review of the service provider's compliance with the Technology Notice before the end of the period for which the Notice has effect or, in the case of a Notice to develop or source technology before the last date by which any step specified in the Notice is required to be taken.[38]

Guidance for Part 3 Providers

A6.27 Ofcom must produce, and publish, guidance for Part 3 service providers about how we propose to exercise our functions under Chapter 5 of Part 7 of the Act (our 'Technology Notice functions') and keep it under review. We must have regard to the guidance when exercising, or deciding whether to exercise, those functions.[39]

Annual Report

A6.28 Ofcom must also produce and publish an annual report about the exercise of our Technology Notice functions and technology which meets, or is in the process of development so as to meet, minimum standards of accuracy. Ofcom must send a copy of our annual report to the Secretary of State, who must lay it before Parliament.[40]

General duties

A6.29 In addition to the specific duties and considerations summarised above, Ofcom has a range of general statutory duties that are relevant to the exercise of its Technology Notice functions.

A6.30 Specifically, when exercising those functions, we will act in accordance with our principal duty under section 3(1) of the Communications Act 2003 ('the Communications Act'):

a) to further the interests of citizens in relation to communications matters; and

b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

A6.31 In performing our principal duty, Ofcom must have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice.[41] In terms of our Technology Notice functions, this means we will take action where it is proportionate and appropriate, but with a willingness to intervene firmly, promptly, and effectively where required. We will always

[37] Section 125(9) of the Act.
[38] Section 126(4) of the Act.
[39] Section 127 of the Act.
[40] Section 128 of the Act.
[41] See section 3(3) of the Communications Act.

seek the least intrusive regulatory methods to achieve our objectives and ensure that interventions are evidence-based, proportionate, consistent, accountable and transparent in both deliberation and outcome, in line with our regulatory principles.

A6.32 In addition, we are required to secure a number of objectives including the adequate protection of citizens from harm presented by content on regulated services, through the appropriate use by providers of such services of systems and processes designed to reduce the risk of such harm.[42] In our work to secure this objective, we must have regard to the matters in section 3(4A) of the Communications Act to the extent they appear to us relevant, which include (among other things):

a) the risk of harm to citizens presented by regulated services;

b) the need for a higher level of protection for children than for adults; and

c) the desirability of promoting the use by providers of regulated services of technologies which are designed to reduce the risk of harm to citizens presented by content on regulated services.

A6.33 Section 3(4) of the Communications Act also sets out other matters to which Ofcom should have regard, including the vulnerability of children and of others whose circumstances appear to put them in special need of protection and the desirability of preventing crime and disorder.

A6.34 As a public authority, Ofcom must also act in accordance with its public law duties to act lawfully, rationally and fairly and, under section 6 of the Human Rights Act 1998, it is unlawful for Ofcom to act in a way which is incompatible with the European Convention on Human Rights ('the ECHR'). Of particular relevance to Ofcom's functions under the Act are the right to freedom of expression (Article 10 ECHR) and the right to privacy (Article 8 ECHR). Other ECHR rights which may also be relevant are the right to freedom of thought, conscience and religion (Article 9 ECHR) and the right to freedom of assembly and association (Article 11 ECHR). In particular, any interference must be prescribed by or in accordance with the law, pursue a legitimate aim and be necessary in a democratic society.

A6.35 In order to be 'necessary', the restriction must be proportionate to the legitimate aim pursued and correspond to a pressing social need. The relevant legitimate aims that Ofcom acts in pursuit of in the context of our functions under the Act include the prevention of crime and disorder, public safety and the protection of health or morals, and the protection of the rights and freedoms of others.[43] In this context, Parliament has legislated for terrorism and CSEA content to be designated as 'priority illegal content' under the Act, requiring service providers to use proportionate systems and processes designed to minimise the length of time for which it is present, and providing for Technology Notices to be issued where necessary and proportionate. This reflects the substantial public interest in limiting the risks of harm to individuals in the UK from this content, and, in relation to CSEA content in particular, the rights of children not to be subject to such abuse and harm.

[42] Section 3(2)(g) of the Communications Act.
[43] Articles 8(2), 9(2), 10(2) and 11(2) ECHR.

A7. Impact Assessments

Policy Impact Assessment

A7.1 Section 7 of the Communications Act requires us to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. In accordance with section 7(4B) of the Communications Act, we have to consider the likely impact on small and micro businesses in relation to proposals connected with our online safety functions. As a matter of policy Ofcom is committed to carrying out and publishing impact assessments in relation to the great majority of our policy decisions, although the form of that assessment will depend on the particular nature of the proposal.

A7.2 The purpose of the policy impact assessment in this Annex is to consider the impact of our proposals in relation to areas where we have, and are proposing to exercise, our regulatory discretion rather than impacts that are unavoidable due to the nature of the duties in the Act. It does not therefore consider the potential impact of Ofcom's power to issue a Technology Notice as this power has been conferred on Ofcom by Parliament and has been subject to impact assessments through the legislative and policy making process. It also does not consider the potential impact from Ofcom being required to give advice to the Secretary of State on minimum standards of accuracy or having to provide guidance to the providers of Part 3 services about how we propose to exercise our Technology Notice functions. We are required by the Act to do so.

A7.3 We do however have discretion in formulating our advice to the Secretary of State on minimum standards of accuracy, and on the substance of our guidance to the providers of Part 3 services. The purpose of this impact assessment is to consider the likely impact from our proposals on these, both of which are set out in this consultation.

A7.4 The scale of the impact will depend on a range of factors. These include, but are not necessarily limited to: the current state of the market for terrorism and CSEA content identification technologies and the scale of interest from that market in seeking accreditation; the extent to which the minimum standards of accuracy ultimately approved and published by the Secretary of State resemble those on which we are consulting; what technology, if any, is ultimately accredited against those standards; and to which services, if any, we issue a Technology Notice.

A7.5 Following consultation, Ofcom expects to provide advice to the Secretary of State regarding minimum standards of accuracy in the detection of terrorism content and CSEA content. It is however ultimately for the Secretary of State to determine the minimum standards of accuracy which are approved and published. Only once these have been published will Ofcom (or a person appointed by Ofcom as relevant) be able to consider whether a particular technology can be accredited as meeting those minimum standards, and if so, whether to issue a Technology Notice to a particular service provider. For this reason, this analysis is unable to estimate the specific impacts to Part 3 regulated services, providers of terrorism and/or CSEA technologies, or the safety outcomes for users of Part 3 services regulated under the Act in aggregate from the policy proposals in this

consultation.[44] We are seeking stakeholder input before issuing final advice to the Secretary of State, and our assessment of impacts here reflects this.

Impact on Part 3 regulated services

A7.6 We do not anticipate that the policy proposals set out in this consultation should have any direct impacts on the providers of Part 3 services, including on small and micro businesses. Accreditation of technology against the minimum standards of accuracy on which we are consulting would not necessarily mean that any regulated service providers are required to use that technology (nor even that we are recommending its use by those providers).

A7.7 Any impacts on specific Part 3 service providers would arise if and when Ofcom is considering issuing a Technology Notice to a particular provider. Before issuing a Technology Notice to a service provider in a particular case however, Ofcom would need to be satisfied that it is necessary and proportionate to require the technology to be used and obtain a skilled person's report to help inform its view. As recognised in our draft guidance for Part 3 service providers, we would therefore consider the costs and impacts of imposing a Technology Notice on a particular Part 3 service provider before issuing a Technology Notice. As explained in Section 2, we are not consulting in this document on the circumstances in which it would be necessary and proportionate to issue a Notice to a particular provider.

A7.8 While we are consulting on draft guidance for the providers of Part 3 services about how Ofcom proposes to exercise its Technology Notice functions, the draft guidance is largely procedural and reflects the framework established by the Act. It is intended to benefit service providers by providing them with transparency on the steps we would expect to follow in making this assessment. The guidance does not in itself impose any additional burdens on the providers of Part 3 services, including small and micro businesses. Rather, by explaining our approach, it is intended to assist providers in understanding how we propose to exercise our Technology Notice functions, and therefore should help to reduce the future burden on them as to what the exercise of those functions might involve. We therefore do not consider we need to separately consider the costs the draft guidance might pose on business.

A7.9 When considering issuing Technology Notices, we will have regard to the regulatory principles of transparency, accountability, proportionality, consistency, and our interventions will be targeted only at cases in which action is needed, as described in paragraph 2.32 of the draft guidance in Annex 5.

Impact on the market for CSEA and/or Terrorism content detection technologies and the impact on technology providers

A7.10 Many of the potential impacts to the market of safety technology providers—including costs, competition, and changes to services – arise at the point of accreditation (and re-accreditation) or at the point of issuing a Technology Notice.

A7.11 We have not considered in detail the costs of the two proposed approaches to setting minimum standards and their associated accreditation process for technology providers, as

[44] This is in line with the Department for Science, Innovation & Technology's Impact Assessment of the Online Safety Act: Online Safety act enactment impact assessment, page 83.

accreditation is optional. We are not compelling technology providers to undertake this process.

A7.12 For the audit-based assessment, we expect that for companies that have followed good software, model development and documentation practices, this process should not be unduly onerous. We welcome views from interested parties on this and would take account of these before finalising our advice to the Secretary of State. We have also developed our proposals regarding minimum standards of accuracy with a view to providing flexible and future-proof standards which should be applicable to the vast range of technologies potentially in scope of this power. The proposals should also be clear and understandable to those seeking accreditation of their technologies, including small and micro businesses.

A7.13 If we proceed with independent performance testing, the responsibility for bearing the costs will be determined at a later date.

Impact on safety outcomes for users of Part 3 services

A7.14 We do not anticipate that the policy proposals set out in this consultation should have any direct impacts on the users of Part 3 services. As noted above, accreditation of technology against the minimum standards of accuracy on which we are consulting would not mean that the providers of any Part 3 services are required to use that technology (nor even that we are recommending its use by those providers).

A7.15 We are also not consulting in this document on the circumstances in which it would be necessary and proportionate to issue a Notice to a particular provider. Any decision on whether it is necessary and proportionate in a particular case would take account (as required by the Act) of the impacts on users, including in relation to freedom of expression within the law and privacy, as well as users' rights to be protected from harm.

A7.16 We recognise that there is a risk that no technologies are accredited. This would mean that we could not issue Technology Notices. However, this risk exists irrespective of the proposals set out in this consultation. Further, we have taken this into account in our policy proposals by seeking to ensure that Ofcom can, if there are suitably accurate technologies, accredit these technologies. We have done this by ensuring that these standards reflect market capabilities and are sufficiently flexible.

A7.17 Further, while a risk nevertheless remains that no technologies are able to meet the standards on which we are consulting, we consider this would likely indicate that no applicants had sufficiently accurate technology. The fact that Ofcom would not be able to require the use of technology in a Technology Notice in that case would be in line with the Act.

Impact on rights

A7.18 As explained in Section 2 and from paragraph A6.34 above, Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way which is compatible with the ECHR. We recognise that the use of terrorism and/or CSEA content detection technologies in practice could have significant impacts on users' rights (including to freedom of expression and to privacy), as well as the rights of others.

A7.19 While accreditation of such technologies would not mean that the providers of any Part 3 services are required to use them, we have considered the way in which our proposals on minimum standards of accuracy and draft guidance could impact these rights:

a) First, our proposals relating to minimum standards of accuracy have been designed to help limit impacts on rights to freedom of expression from accredited technologies. We propose that the audit-based assessment include a range of objectives. Some of these, for example, concern reproducible performance, robust data labelling processes, as well as bias identification and mitigation, which should help reduce the risk of accredited technologies falsely flagging content as illegal content. Further, the supplementary independent performance testing stage that we propose is designed to ensure that only the higher performing technologies of those submitted for accreditation are accredited.

b) Second, our proposals relating to minimum standards of accuracy have also been designed with users' rights to privacy in mind. One of the objectives in the audit-based assessment, for example, is that the technology has been developed in a secure environment, with sufficient cybersecurity, privacy and data protection measures in place. We have also explained in Section 4 that Ofcom, or a nominated third party, would reserve the right to not consider a technology against the minimum standards of accuracy. This would be where it is found by a Court or other competent authority (such as the ICO) to have been developed in breach of UK data protection or other legal requirements.

c) Third, while the draft guidance for Part 3 service providers is procedural in nature, it explains that Ofcom will have careful regard to rights impacts, taking account of all the available evidence and on a case-by-case basis, before issuing a Technology Notice.

    i) While not required by the Act, it recognises that we would typically expect to consider users' rights to freedom of expression, and the risk of an accredited technology resulting in a breach of any relevant statutory provision or rule of law concerning privacy, before issuing a Technology Notice relating to the development or sourcing of technology.

    ii) It also recognises that other ECHR rights may be relevant before issuing a Technology Notice. These include for example, the right to freedom of thought, conscience and religion and the right to freedom of assembly and association, as well as the right to privacy of victims of child sexual abuse and to the protection of their personal data.

    iii) The guidance provides transparency about how we will approach our assessment of whether a Technology Notice is necessary and proportionate. It explains that we would carefully consider the precise requirements that are imposed in any particular case, including the kinds of content or parts of the service on which any accredited technology is required to be used, and the wider systems and processes that might be required, such as complaints and human moderation. It also explains that we would consider whether independent compatibility testing is appropriate to inform our assessment.

Equality legislation and Welsh language

A7.20 Ofcom is also subject to duties under the Equality Act 2010 ('the EA 2010'). This includes the public sector equality duty set out in section 149, which requires Ofcom, in the exercise of our functions, to have due regard to the need to:

a) eliminate discrimination, harassment, victimisation and any other conduct that is prohibited by or under the EA 2010;

b) advance equality of opportunity between persons who share a 'relevant protected characteristic' and persons who do not share it; and

c) foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

A7.21 The relevant protected characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

A7.22 In addition, section 75 of the Northern Ireland Act 1998 requires us to promote good relations between people sharing specified characteristics, including people of different religious beliefs, political opinions or racial groups.

A7.23 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards in relation to the use of Welsh.

A7.24 Equality Impact Assessment

A7.25 We have given careful consideration to whether our policy proposals will have a particular impact on persons sharing protected characteristics (broadly including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. This assessment helps us comply with our duties under the EA 2010 and the Northern Ireland Act 1998.[45]

A7.26 Ofcom do not expect that these policy proposals will have an adverse impact on persons sharing protected characteristics as we are not requiring the use of any technologies as part of these policy proposals.

A7.27 Further, fairness is one of the assessment principles we are proposing to include within our proposals regarding minimum standards of accuracy. To this extent, our proposals should further the interests of persons with protected characteristics.

A7.28 We would also expect to consider equality impacts as part of any decision on whether it is necessary and proportionate to issue a Technology Notice to a particular provider, and what requirements should be imposed in that case.

A7.29 Welsh Language Impact Assessment

A7.30 The Welsh language has official status in Wales. To give effect to this, certain public bodies, including Ofcom, are required to comply with Welsh language standards.[46] Accordingly, we have considered:

a) The potential impact of our policy proposals on opportunities for persons to use the Welsh language;

b) The potential impact of our policy proposals on treating the Welsh language no less favourably than the English language; and

[45] Section 75 of the Northern Ireland Act 1998

[46] The Welsh language standards with which Ofcom is required to comply are available on our website.

c) How our proposals could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A7.31 We do not expect the policy proposals we are consulting on in this document to have any adverse effect on the Welsh language, nor do they treat the Welsh language less favourably than the English language. We are also not persuaded that it would be appropriate or proportionate for Ofcom to formulate its policy proposals to have a positive impact on the Welsh language, for example, by including accuracy in the Welsh language as a specific standard within the minimum standards of accuracy.

A7.32 We note however that we are proposing to ask those applying for accreditation to include details about the different languages supported by the technology. This would be used to inform any subsequent decisions on whether it is necessary and proportionate to require the use of that technology in a Technology Notice, and the requirements that might be included in that Notice.

A8. Glossary

A8.1 This glossary defines the terms we have used throughout this document.

Term	Definition
Accreditation scheme	A process to be set up by Ofcom which enables technologies to be assessed (by Ofcom or another person appointed by Ofcom) against the minimum standards of accuracy.
Accredited technology	Technology that has been accredited by Ofcom (or another person appointed by Ofcom) as meeting the minimum standards of accuracy.
Act	The Online Safety Act 2023.
Benign content or data	In the context of this consultation, benign data is information that is not categorised as terrorism or CSEA content. It may still include data or content that is otherwise categorised as harmful.
Codes of Practice (Codes)	The set of measures recommended by Ofcom for compliance with certain online safety duties, including the illegal content safety duties. Ofcom is required to prepare Codes of Practice under section 41 of the Act. Our draft Illegal Content Codes of Practice for user-to-user services and search services (as submitted to the Secretary of State) have been published at the same time as this document.
Combined service	A regulated user-to-user service that includes a public search engine.
Content	Anything communicated by means of an internet service, whether publicly or privately, including written material or messages, oral communications, photographs, videos, visual images, music and data of any description.
CSAM (child sexual abuse material)	A category of CSEA content, including in particular indecent or prohibited images of children (including still and animated images, and videos, and including photographs, pseudo-photographs and non-photographic images such as drawings). CSAM also includes other material that includes advice about grooming or abusing a child sexually or which is an obscene article encouraging the commission of other child sexual exploitation and abuse offences. Furthermore, it includes content which links or otherwise directs users to such material, or which advertises the distribution or showing of CSAM.

Term	Definition
CSAM URL	For the purposes of Ofcom's first Illegal Content Codes of Practice, this means a URL at which CSAM is present, or a domain which is entirely or predominantly dedicated to CSAM (and for this purpose a domain is 'entirely or predominantly dedicated' to CSAM if the content present at the domain, taken overall, entirely or predominantly comprises CSAM, such as indecent images of children, or content related to CSEA content).
CSEA (Child Sexual Exploitation and Abuse)	Refers to offences specified in Schedule 6 to the Act, including offences related to CSAM and grooming. CSEA includes but is not limited to causing or enticing a child or young person to take part in sexual activities, sexual communication with a child and the possession or distribution of indecent images. This is discussed in more detail from paragraph 2.12 of this document.
CSEA content	Refers to content that amounts to an offence specified in Schedule 6 to the Act.
Data labelling	Data labelling is the process of identifying raw data (such as, images, text, videos, etc.) and adding one or more meaningful and informative labels to provide context. References to data labelling, labels and labelling data should be construed accordingly.
Deployment	For the purpose of this consultation, this refers to an operational technology being put into use (or being considered for use) on a particular internet service. References to deploy shall be construed accordingly.
ECHR	The European Convention on Human Rights (incorporated into domestic law by the Human Rights Act 1998).
Encounter	In relation to content, means read, view, hear or otherwise experience content.
F1 Score	This is the harmonic mean of precision and recall and provides a single measure of a model's accuracy that balances both false positives and false negatives. It is calculated as the product of precision and recall divided by the sum of precision and recall, multiplied by two. For the meaning of 'precision', 'recall', 'false positive' and 'false negative' see Annex 12 of this document.

Term	Definition
Hash	For the purposes of this consultation, this means a hash value. This is a digital footprint of content, which can be used together with a hash-matching algorithm to identify content that has that same or a similar digital footprint. A hash is distinct from the content to which it relates.
Hash-matching / Hashing	This is a type of technology which can be used as a content moderation tool, including to detect illegal content. Broadly speaking, it is a process for detecting when users attempt to upload content which has previously been identified as being illegal or otherwise violative. It allows services to prevent the re-upload of illegal content. It involves matching a hash of a unique piece of known illegal content stored in a database with user-generated content. Hashing is an umbrella term for techniques to create fingerprints of files on a computer system. An algorithm known as a hash function is used to compute a hash from a file. Hash matching can be used to prevent the upload, download, viewing or sharing of illegal or harmful content.
Illegal content	Content which amounts to a relevant offence. Content amounts to a relevant offence if: (a) the use of that content (i.e., words, images, speech or sounds) amounts to a relevant offence; (b) the possession, viewing or accessing of the content constitutes a relevant offence; or (c) the publication or dissemination of the content constitutes a relevant offence.
Illegal content safety duties	The duties in section 10 of the Act (user-to-user services) and section 27 of the Act (search services).
Illegal harm	Harms arising from illegal content and the commission and facilitation of priority offences.
Internet service	A service that is made available by means of the internet. This includes where it is made available by means of a combination of the internet and an electronic communications service ('Electronic communications service' has the same meaning as in section 32(2) of the Communications Act 2003).

Term	Definition
Keyword matching	This is a type of technology which can be used as a content moderation tool, including to detect illegal content. Broadly speaking, it can involve a process of matching words and/or phrases to words and/or phrases previously identified as indicative of a particular harm or offence.
Metadata	For the purpose of this consultation, this is a set of data that describes and gives information about other data used for content moderation.
Metrics	For the purpose of this consultation, metrics refers to the performance metrics against which Ofcom are proposing to calculate benchmarked thresholds as part of a supplementary independent performance testing stage. If this stage is included in the minimum standards of accuracy, the performance of technologies submitted for accreditation would be evaluated against these metrics. Annex 12 provides more detail on the specific metrics we are proposing should be considered and for which benchmarked thresholds should be calculated.
Minimum standards of accuracy	Refers to the standards approved and published by the Secretary of State relating to the detection of terrorism and CSEA content, following advice from Ofcom.
Part 3 service	Refers to a regulated user-to-user service or a regulated search service.
Priority illegal content	Content which amounts to a priority offence.
Priority offences	The offences set out in Schedules 5 (Terrorism offences), 6 (CSEA offences) and 7 (Priority offences) to the Act.
Proactive technology	This consists of three types of technology: content identification technology, user profiling technology, and behaviour identification technology (subject to certain exceptions), as defined in section 231 of the Act.

Term	Definition
Provider	The provider of a user-to-user service, or search service, is to be treated as being the entity that has control over who can use the user-to-user part of the service, or the operations of the search engine (and that entity alone). The provider of a combined service is to be treated as the entity that has control over both who can use the user-to-user part of the service and the operations of the search engine (and that entity alone). If no entity has such control but an individual or individuals do, the provider of the service is to be treated as being that individual or those individuals.
Regulated search service	An internet service that is, or includes, a search engine. Such services will only be 'regulated' if they have 'links with the United Kingdom' and do not fall within Schedule 1 or Schedule 2 to the Act – see section 4(2) of the Act for more detail.
Regulated user-to-user service	An internet service through which content that is generated, uploaded or shared by users may be encountered by other users of the service. Such services will only be 'regulated' if they have 'links with the United Kingdom' and do not fall within Schedule 1 or Schedule 2 to the Act – see section 4(2) of the Act for more detail.
Relevant content	Terrorism content or CSEA content or both those kinds of content (depending on the kind, or kinds, of content in relation to which the specified technology is to operate).
Relevant non-priority illegal content	Content which amounts to a relevant non-priority offence.

Term	Definition
Relevant non-priority offence	Offences under UK law which are not priority offences under Schedules 5, 6 or 7 to the Act, where: a. The victim or intended victim of the offence is an individual (or individuals); b. The offence is created by the Online Safety Act, another Act, an Order in Council or other relevant instrument. The effect of this is that offences created by the UK courts are not relevant non-priority offences, and offences created in the devolved Parliaments or Assemblies are only relevant non-priority offences if certain procedures are followed in their making; c. The offence does not concern the infringement of intellectual property rights, the safety or quality of goods, or the performance of a service by a person not qualified to perform it; and d. The offence is not an offence under the Consumer Protection from Unfair Trading Regulations 2008.
Relevant offences	All priority offences and relevant non-priority offences.
Search	Search by any means, including by input of text or images or by speech, and references to a search request are to be construed accordingly.
Search content	Content that may be encountered in or via search results of a search service. It does not include paid-for advertisements, news publisher content, or content that reproduces, links to, or is a recording of, news publisher content. Content encountered 'via search results' includes content encountered as a result of interacting with search results (for example, by clicking on them) and does not include content encountered as a result of subsequent interactions.
Search engine	A service or functionality which enables a person to search some websites or databases but does not include a service which enables a person to search just one website or database.

Term	Definition
Search results	Content presented to a user of a search service (or a user-to-user service that includes a search engine) by operation of the search engine in response to a search request made by the user.
Search service	An internet service that is, or includes, a search engine.
Skilled person	A person appearing to Ofcom to have the skills necessary to prepare a report about matters that Ofcom considers to be relevant. A skilled person could be an individual, a firm or an organisation.
Skilled person's report	A report prepared by a skilled person about matters that Ofcom considers to be relevant. Ofcom is required to obtain a skilled person's report before issuing a Technology Notice.
Systems and/or processes	Refers to human or automated systems and/or processes, and accordingly includes technologies.
Taking down (content)	Refers to any action that results in content being removed from a user-to-user service or being permanently hidden so users of the service cannot encounter it (and related expressions are to be read accordingly).
Target content	Refers, for content moderation purposes, to the kind (or kinds) of content that a technology is being used to detect. In the case of a Technology Notice, the target content would be terrorism content or CSEA content (or both).
Technology Notice (Notice)	Refers to a notice under section 121 of the Act requiring a provider of a Part 3 service to use: (a) accredited technology to deal with terrorism or CSEA content, or both, or (b) best endeavours to develop or source technology to deal with CSEA content.
Technology Notice functions	Ofcom's functions under Chapter 5 of Part 7 of the Act.
Terrorism content	An offence specified in Schedule 5 to the Act, including but not limited to offences relating to proscribed organisations, encouraging terrorism, training and financing terrorism. This is discussed in more detail from paragraph 2.10 of this consultation.
Terrorism/CSEA content detection technology	Technology to identify and prevent users encountering user-generated terrorism content or CSEA content, and/or to identify search content that is terrorism content or CSEA content.

Term	Definition
Testing category	Refers to the grouping of technologies that pass the audit-based assessment for the purposes of conducting testing (and setting benchmarked thresholds) in the supplementary, independent performance testing stage. Ofcom propose that technologies be categorised based on: a) whether they identify terrorism content or CSEA content, and b) what data they analyse (e.g., hashes, images, text).
URL (Uniform Resource Locator)	A reference that specifies the location of a resource accessible by means of the internet.
URL detection	This is a type of technology which can be used as a content moderation tool. Broadly speaking, it can involve a process of matching URLs to URLs previously identified as hosting illegal or harmful content on other services.
User data	Data provided by users, including personal data (e.g., data provided when a user sets up an account), or created, compiled or obtained by providers of regulated services and relating to users (e.g., data relating to when or where users access a service or how they use it).
User-generated content	Content (a) that is: (i) generated directly on the service by a user of the service, or (ii) uploaded to or shared on the service by a user of the service, and (b) which may be encountered by another user, or other users, of the service by means of the service.
User-to-user part (of a service)	In relation to a user-to-user service, means the part of the service on which content that is user-generated content in relation to the service is present.
User-to-user service	An internet service through which content that is generated, uploaded or shared directly on the service by users may be encountered by other users of the service.
Warning Notice	Refers to a notice given to the provider of a Part 3 service under section 123 of the Act which explains that Ofcom intends to issue a Technology Notice. The provider may make representations to Ofcom on the Warning Notice. Ofcom is required to give a Warning Notice before it can issue a Technology Notice.

Term	Definition
Withheld dataset	Refers to a set of data that is intentionally kept separate and not used during the development of technology, but reserved for later use to evaluate the technology's performance and ensure it generalises well to new, unseen data.