Technology Notices to deal with terrorism and/or CSEA content

Annex 5: Draft Guidance on the exercise of Ofcom's functions under Chapter 5 of Part 7 of the Online Safety Act 2023

Consultation

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

Contents

Annex

A1. Overview

A1.1 Ofcom is the independent regulator for online safety in the UK. The Online Safety Act 2023 ('the Act') provides that terrorism content and Child Sexual Exploitation and Abuse ('CSEA') content are both categories of priority illegal content, and Ofcom has been given a range of powers and duties to address such content.

A1.2 Part 7 of the Act sets out Ofcom's powers and duties in relation to regulated services. These include a duty to prepare and issue Codes of Practice for providers of regulated user-to-user and search services1 describing measures recommended for compliance with their online safety duties (including in respect of terrorism and CSEA content), and powers to take enforcement action when they are not in compliance. We refer to regulated user-to-user and search services as 'Part 3 services' or 'services' in this guidance.

A1.3 In addition, Chapter 5 of Part 7 of the Act gives Ofcom the power, where we consider it necessary and proportionate, to issue a notice to the provider of a Part 3 service to deal with terrorism content and/or CSEA content (we refer to such notices in this guidance as a 'Technology Notice' or 'Notice').[2]

A1.4 Ofcom is required by the Act to produce guidance for providers of Part 3 services about how we propose to exercise our functions under that Chapter (our 'Technology Notice functions').3 This guidance has been produced pursuant to that duty.

[1] 'User-to-user service' and 'search service' are defined in section 3 of the Act. A service will be regulated for the purposes of the Act if it has links with the UK and does not fall within Schedule 1 or Schedule 2 of the Act (see section 4 of the Act).

[2] Ofcom's power to issue a notice is set out in section 121 of the Act.

[3] Section 127(1) of the Act.

A2. Introduction

A2.1 Chapter 5 of Part 7 of the Act gives Ofcom the power, where we consider it necessary and proportionate, to issue a Technology Notice requiring a provider of a Part 3 service ('service providers')[4] to use:

a) accredited technology to deal with terrorism or CSEA content, or both ('relevant content');[5] or;
b) best endeavours to develop or source technology to deal with CSEA content.

A2.2 This guidance sets out how Ofcom will typically approach the exercise of our Technology Notice functions.

The scope of this guidance

A2.3 This guidance is for service providers and is intended to provide procedural guidance regarding the steps Ofcom would expect to take, and the matters it would expect to consider, when exercising (and deciding whether to exercise) our Technology Notice functions.

What does this guidance cover?

A2.4 This Section summarises the relevant legal framework, including the requirements that we can impose in a Technology Notice.

A2.5 The remainder of this guidance is structured as follows:

- **Section A3** outlines how we will approach our assessment of whether it is necessary and proportionate to issue a Technology Notice, including the matters we must consider under the Act and other matters or considerations that might be relevant to our decision.
- **Section A4** explains what might prompt us to initially consider exercising our Technology Notice functions, including how we might consider our power to issue a Technology Notice as part of our standard 'initial assessment' process, and the potential outcomes of an initial assessment.
- **Section A5** outlines what service providers can typically expect when we are considering issuing a Technology Notice, including how we will engage with the service provider, and our approach to information gathering (such as obtaining a skilled person's report).
- **Section A6** explains the stages of our process from deciding whether to issue a Warning Notice, including giving the service provider an opportunity to make representations, to deciding whether it is necessary and proportionate to issue a Technology Notice.

[4] Or a combined service, which is defined in section 4(7) of the Act as a regulated user-to-user service that includes a public search engine.
[5] In this guidance, when referring to terrorism and/or CSEA content (as appropriate) we use the term 'relevant content'.

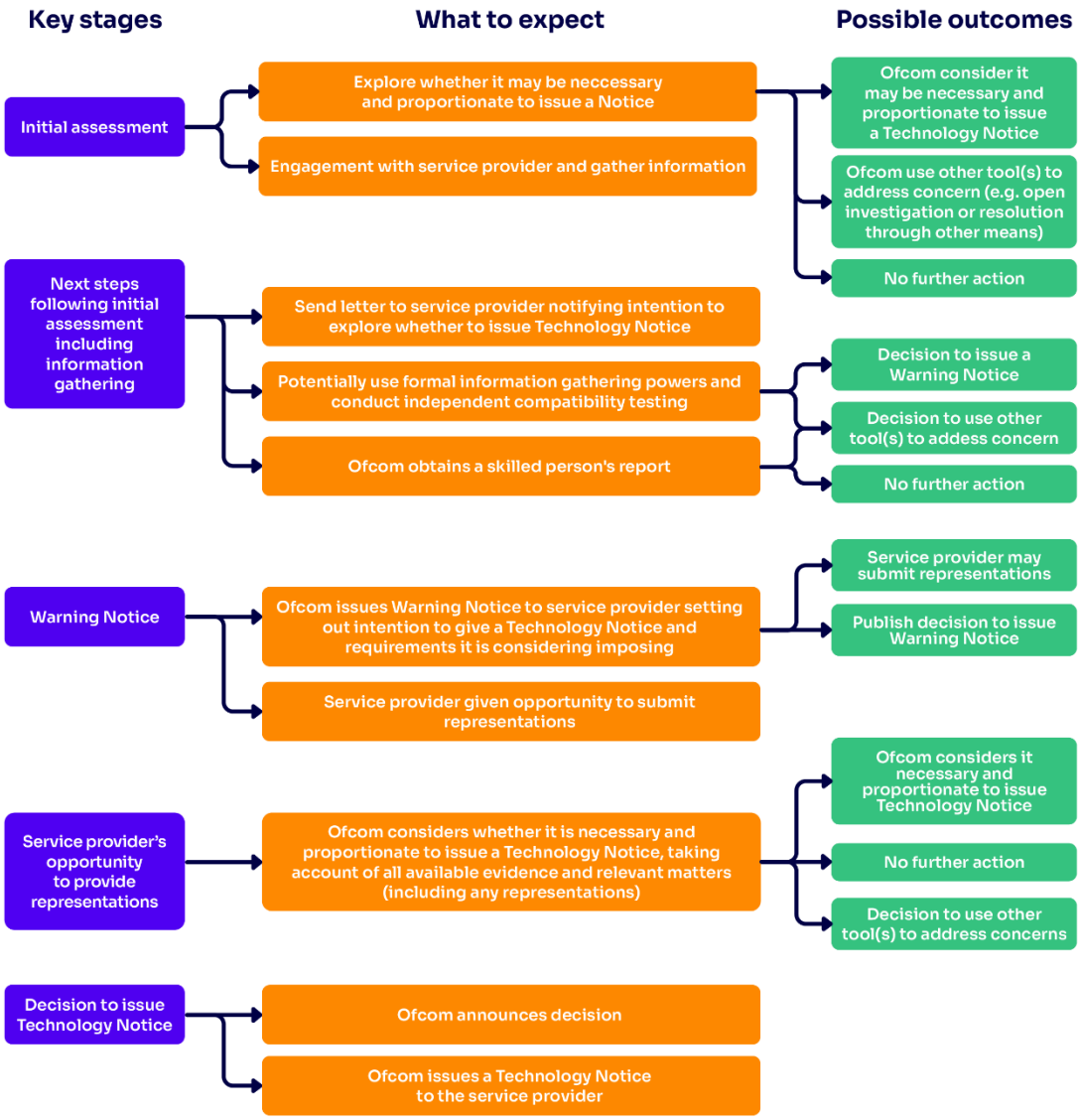
- **Section A7** explains the next steps following a Technology Notice being issued to a service provider, including reviewing their compliance with the Notice and the consequences of non-compliance.
- **Section A8** outlines how we expect to approach the disclosure of information and publication about the exercise of our Technology Notice functions.

A2.6 This guidance **does not** cover the process that Ofcom (or a third party appointed by Ofcom) will take to accredit technologies for the purpose of our Technology Notice functions (see paragraph A2.22).

A2.7 This guidance **does not** apply to the criminal enforcement of offences under the Act and **does not** set out our approach to the exercise of our enforcement powers. It will, however, refer to Ofcom's Online Safety Enforcement Guidance ('OS Enforcement Guidance'), where relevant.

A2.8 The key stages of the process when exercising our Technology Notice functions within the legal framework outlined in this guidance, a summary of what to expect, and possible outcomes during each stage are set out in **Figure A1 below**.

Figure A1: Process for exercising Technology Notice functions



The status of this guidance

A2.9 This guidance sets out Ofcom's general approach to exercising our Technology Notice functions under the Act, including the typical process we will follow for issuing a Notice. In exercising these functions, or deciding whether to exercise them, we must have regard to this guidance.[6] Where we depart from the approach set out in the guidance, we will explain our reasons for doing so.

A2.10 The guidance is not a substitute for any regulation or law and is not legal advice.

A2.11 We will keep this guidance under review and amend it as appropriate in light of further experience, developing law and practice and any change to Ofcom's powers and responsibilities.

[6] Section 127(5) of the Act.

Other relevant publications

A2.12 Ofcom has a suite of relevant publications that readers may also find useful, and to which we refer in this guidance. These include:

- **Ofcom's OS Enforcement Guidance** which sets out how Ofcom will typically approach enforcement under the Act.[7] Ofcom's power to issue a Technology Notice is complementary to our enforcement powers, and we do not need to have identified a compliance concern or open an enforcement investigation before exercising, or deciding whether to exercise, our Technology Notice functions.
- **Ofcom's [draft] Online Safety Information Powers Guidance** ('[draft] OS Information Powers Guidance'), which explains our information gathering powers under the Act, when and how we might use each power, regulated services' obligations in relation to those powers, and potential consequences of non-compliance.[8]
- **Ofcom's Online Safety Guidance on Judgement for Illegal Content**, which sets out the process that services may follow to determine if there are reasonable grounds to infer that a piece of content is illegal.[9]
- **Ofcom's Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act**.[10] This is intended to assist the providers of regulated user-to-user services that are looking to comply with their online safety duties by taking measures set out by Ofcom in a Code of Practice which relate specifically to content communicated 'publicly'. However, the concept of content communicated 'publicly' and 'privately' is also relevant to Ofcom's Technology Notice functions, and this guidance may therefore help service providers understand Ofcom's approach to these concepts more generally (see paragraph A2.21).

A2.13 This guidance **does not** cover service providers' compliance with data protection law. The regulator for data protection is the Information Commissioner's Office ('ICO'), which has a range of guidance service providers may consult for information about how they can comply with data protection law.[11]

[7] Ofcom, Online Safety Enforcement Guidance [accessed 16 December 2024].
[8] Ofcom, [draft] Online Safety Information Powers Guidance [accessed 16 December 2024].
[9] Ofcom, Online Safety Guidance for Judgement on Illegal Content [accessed 16 December 2024], which includes terrorism and CSEA content. See also footnote 12.
[10] Ofcom, Guidance on content communicated publicly and privately under the Online Safety Act [accessed 16 December 2024]. See also footnote 17.
[11] In particular, please refer to its guidance on Online safety and data protection | ICO; Age appropriate design | ICO; and further guidance For organisations | ICO [accessed 16 December 2024].

Relevant legal framework

What is terrorism and CSEA content?

A2.14 Terrorism content and CSEA content are both categories of 'priority illegal content' under the Act.[12] These are the most serious categories of content covered by the Act, and all providers will need to act to prevent users encountering such content.

A2.15 Terrorism content refers to content which amounts to an offence specified in Schedule 5 of the Act. These offences include, but are not limited to:

a) A series of offences relating to 'proscribed organisations';
b) Offences related to information likely to be of use to a terrorist;
c) Offences relating to training for terrorism; and
d) Other offences involving encouraging terrorism or disseminating terrorist materials.

A2.16 CSEA content refers to content which amounts to an offence specified in Schedule 6 of the Act. These offences include, but are not limited to:

a) Offences relating to the making, showing, distributing or possessing of an indecent image or film of a child;
b) Linking to or directing a user to child sexual abuse material (CSAM);
c) An offence of possession of a paedophile manual;
d) Sexual activity offences (potential victim under 16); and
e) Adult to child offences (potential victim under 16).

What Ofcom can require in a Technology Notice

A2.17 The Act provides Ofcom with the power,[13] if we consider it necessary and proportionate, to give a Technology Notice to a service provider requiring it to:

a) use **accredited technology** to deal with terrorism content and/or CSEA content; or
b) use best endeavours to **develop or source technology** which meets minimum standards of accuracy to deal with CSEA content.

A2.18 For a Notice requiring the use of **accredited technology**:

a) user-to-user services may be required to use that technology to identify and swiftly take down, or prevent individuals from encountering, terrorism and/or CSEA content; and
b) search services may be required to use that technology to identify search content of the service that is terrorism and/or CSEA content and swiftly take measures to secure that, so far as possible, search content no longer includes such content identified by the technology.[14]

[12] Section 59(3) of the Act sets out when content amounts to an offence. Section 192 of the Act sets out how, where they are required to do so, providers of services should make judgements as to whether content is illegal content. The approach set out in the Act is such that 'illegal content judgements' are to be made if the service provider has 'reasonable grounds to infer' that the content in question amounts to a relevant offence. See also Online Safety Guidance for Judgement on Illegal Content.
[13] Section 121(1) of the Act.
[14] Section 121(2)(a) of the Act and section 121(3)(a) of the Act. See also section 57(2), which defines 'search content'.

A2.19 For a Notice relating to the **development or sourcing of technology**, services may be required to use **best endeavours** to develop or source technology, which meets minimum standards of accuracy, that can be used:

a) in the case of user-to-user services, to identify and swiftly take down, or prevent individuals encountering, CSEA content; and
b) in the case of 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.[15]

A2.20 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 the search engine function of the service.[16]

A2.21 For 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; and to use accredited technology to address **terrorism content communicated publicly** by means of the service.[17]

A2.22 Where we refer to **accredited technology**, we mean technology that has been accredited by Ofcom (or a third party appointed by Ofcom) as meeting minimum standards of accuracy in the detection of relevant content. The minimum standards of accuracy are standards approved and published by the Secretary of State, following advice from Ofcom.[18]

A2.23 We may impose requirements in a Technology Notice only in relation to the design and operation of a service in the UK, or as it affects UK users of the service.[19]

Additional requirements

A2.24 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]

A2.25 If a service provider is already using accredited technology in relation to the service, we may require that service provider to **use the accredited technology more effectively**.[21]

A2.26 A Technology Notice may also require the service provider to **operate an effective complaints procedure.**[22]

---

[15] Section 121(2)(b) of the Act and section 121(3)(b) of the Act.
[16] Section 121(4) of the Act.
[17] Section 232 of the Act specifies factors that we must particularly consider when deciding whether content is communicated 'publicly' or 'privately' for the purposes of a Notice to deal with terrorism content. These are: 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'.
[18] Section 125(12) and (13) 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. See also paragraph A6.5(b) below.
[22] Section 125(3) and (4) of the Act. See also paragraph A6.5(b) below.

Timescales for compliance and review of a Technology Notice

A2.27 In the case of a Technology Notice to **use accredited technology**, we must specify the period within which the requirements imposed by the Notice will have effect. This may be for up to **36 months**, which begins from the last day of the period specified in the Notice for the service provider to take the action required to comply with the Notice. We must also specify a reasonable period for compliance with the notice.[23]

A2.28 Where we issue a Technology Notice requiring a service provider to **develop or source technology**, the Notice must specify a reasonable period within which each of the steps specified in the Notice must be taken.[24]

A2.29 In addition, 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.[25]

What Ofcom must do before issuing a Technology Notice

A2.30 Before we may issue a Technology Notice, Ofcom is required to:

a) **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 ('skilled person's report') (see paragraphs A5.11 to A5.13);[26]
b) give a **Warning Notice** to the service provider, which includes providing them with the opportunity to make representations to Ofcom on our intention to issue a Notice (see paragraphs A6.5 to A6.6);[27] and
c) be satisfied that it is **necessary and proportionate** to issue the Technology Notice. The Act specifies a number of matters we must consider, in particular, when making our decision.[28] These matters are outlined in Section A3.

Ofcom's general duties

A2.31 When exercising our Technology Notice functions, we will act in accordance with our principal duty under section 3(1) of the Communications Act 2003 ('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.

A2.32 In performing our principal duty, we must have regard to the principles under which our 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.[29] 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 seek the least

[23] Section 125(6)(f) and (7) of the Act (see also section 125(6)(e)).
[24] Section 125(8)(d) of the Act.
[25] Section 126(4) of the Act.
[26] Section 122 of the Act. See also section 104(3) and (4).
[27] Section 123 of the Act.
[28] Section 124 of the Act.
[29] Section 3(3) of the Communications Act.

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.

A2.33 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.[30] 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 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.

A2.34 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.

A2.35 As a public authority, we must also act in accordance with our public law duties to act lawfully, rationally and fairly and, under section 6 of the Human Rights Act 1998, it is unlawful for us to act in a way which is incompatible with the European Convention on Human Rights ('the ECHR'). Of particular relevance to our 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.

A2.36 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.[31] 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.

[30] Section 3(2)(g) of the Communications Act.
[31] As set out in Articles 8(2), 9(2), 10(2) and 11(2) of the ECHR.

A3. How we approach our decision to issue a Technology Notice

Introduction

A3.1 We can only issue a Technology Notice where we consider that it is necessary and proportionate to do so. The matters we must particularly consider when making this assessment are set out in the Act, although there may be other relevant factors which we consider.

A3.2 In this Section we outline how we will approach our assessment of whether it is necessary and proportionate to issue a Technology Notice, including the matters we must consider under the Act, and other matters or considerations that might be relevant to our assessment.

A Technology Notice must be necessary and proportionate

A3.3 We will decide whether it is necessary and proportionate to issue a Technology Notice on a case-by-case basis. In making this assessment, we will take account of:

a) the matters set out in section 124(2) of the Act (the 'Specified Matters'); and
b) any other factors we consider relevant in the circumstances.

A3.4 Any decision as to whether a Technology Notice is necessary and proportionate in a particular case would be highly fact-specific and would be taken in the round, considering all the Specified Matters (where applicable) and any other factors we consider relevant in the circumstances. Even if we consider it necessary and proportionate to issue a Notice to one service provider, and the nature of our concerns in relation to another service are very similar (for example, about the prevalence of CSEA imagery on a service), it does not follow that we would consider it to be necessary and proportionate for us to require the use of that same technology (or any accredited technology) on that other service.

The matters we must consider when deciding if a Technology Notice is necessary and proportionate

A3.5 The Specified Matters, which we must particularly consider when deciding whether it is necessary and proportionate to issue a Technology Notice to a service provider, are:

a) the kind of service it is;
b) the **functionalities** of the service;[32]
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;

[32] 'Functionality' is defined in section 233 of the Act.

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;[33]
g) the **systems and processes** used by the service which are designed to identify and remove relevant content;[34] and
h) the contents of the **skilled person's report** obtained.[35]

A3.6 Where we are considering issuing a Technology 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;[36]
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);
c) 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:

i) have an adverse impact on the **availability of journalistic content**[37] on the service; or

ii) result in a breach of the **confidentiality of journalistic sources**; and

d) 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.

A3.7 We set out below some high-level observations on the Specified Matters:

a) The Act does not provide that any one of the Specified Matters carries any greater weight than another, and it is not an exhaustive list.
b) With regards to our consideration of the **level of risk of harm** and its **severity**, we expect to be guided by our Register of Risks, as this sets out our assessment of where and how illegal harms manifest online and the factors that give rise to risks of harm.[38]
c) When considering the extent of any anticipated interference with **users' right to freedom of expression and privacy**, we would expect to have regard to evidence regarding the false positive rate of the technology under consideration.[39] This is because flagging of false positives could result in users incorrectly having their content removed, their account banned or suspended, or being reported to the National Crime Agency (NCA) or other organisations, which would represent a potentially significant impact on their rights to freedom of expression and privacy. However, we do not expect to

[33] See section 234 of the Act for the meaning of 'harm'.
[34] 'Systems and/or processes' refers to human or automated systems and/or processes, including technologies (section 236(1) of the Act).
[35] As required by section 122 of the Act.
[36] 'Freedom of expression' means the freedom to receive and impart ideas, opinions or information (Article 10(1) of the ECHR by means of speech, writing or images (section 236(1) of the Act).
[37] See section 19 of the Act for the meaning of 'journalistic content'.
[38] Ofcom, Register of Risks [accessed 16 December 2024].
[39] In the context of detecting relevant content, a false positive is a case where the technology has incorrectly identified content as terrorism content or CSEA content.

consider this in isolation and would bear in mind any other relevant information, such as:

i) the nature of the content that is incorrectly detected by the technology as relevant content, particularly whether it is still illegal content or whether it is afforded a greater degree of protection by the law (such as political speech);

ii) and any potential safeguards to mitigate the risk, such as the layering of measures (for example, the use of human moderators together with the accredited technology to review some or all detected content).

d) If Ofcom is concerned about terrorism content on a service, when considering the **prevalence of relevant content** on (and the extent of its dissemination by means of) the service we would expect to focus in particular on the prevalence and dissemination of terrorism content communicated publicly. This is because our power to issue a Technology Notice to deal with terrorism content is limited to content communicated publicly. However, where we have evidence that terrorism content is prevalent or disseminated on private communications, this may still be relevant to our consideration of whether it is necessary and proportionate to issue a Notice.

e) In considering whether the use of any **less intrusive measures** would be likely to achieve a significant reduction in the amount of relevant content, we would take into consideration the other tools available to us to resolve the issue (see Section A4). These may include opening an investigation into the service provider's compliance with its online safety duties, which could lead to us issuing a decision that a regulatory breach has taken place, and imposing financial penalties and other sanctions, including a requirement to use proactive technology.[40]

f) In the case of a Technology Notice to **develop or source technology**, while we are not required to consider the matters set out at paragraph A3.6 above we would typically expect to do so, as we think that it is important we consider any potential impacts on users' rights to freedom of expression and privacy and the availability of journalistic content or sources, and whether the use of any less intrusive measure would be likely to achieve a reduction in the amount of relevant content, were the service provider to ultimately use the technology that it has developed or sourced. However, we would have to assess this based on the information available to us at that time given that we would not have a specific technological solution in mind at this stage.

Other matters we are likely to consider

A3.8 Whilst we are not required by the Act to consider any factors other than the Specified Matters, we would generally expect the following to also be relevant to our consideration of whether it is necessary and proportionate to issue a Technology Notice requiring the use of accredited technology or requiring technology to be sourced or developed:

a) The **technical feasibility** for the service provider of doing what would be required of them in the Technology Notice, taking into account the way the service is configured. However, we note that, for a Notice requiring the use of accredited technology, we would not be restricted from considering a technical solution technically feasible on the grounds that proportionate changes would be required to be made to the design and/or

[40] See Section 6, paragraphs 6.51 to 6.53 of Ofcom's OS Enforcement Guidance - the use of proactive technology can be required in a confirmation decision. We note that we may open an investigation alongside the exercise of our Technology Notice functions (see paragraph A4.11 below).

operation of the service for the technology to be used effectively (see paragraph A2.24 above).

b) The **size and capacity**[41] of the service provider. For example, if a service provider would need to use accredited technology together with human moderators to comply with the Technology Notice, we would expect their size and/or capacity to be relevant to our consideration of whether it would be proportionate in the circumstances, especially where extensive human review of detected content may be required.

c) The likely **financial cost** to the service provider of complying with the Technology Notice. This would include, in the case of a Notice requiring the use of accredited technology, the price payable by the service provider to use the technology for the period required by the Notice.

d) Any impact on **other rights** protected by the ECHR. Whilst the Act specifically requires us to have particular regard to users' right to freedom of expression and any relevant statutory provision or rule of law concerning privacy when considering whether it is necessary and proportionate to issue a Technology Notice requiring a service provider to use accredited technology, other ECHR rights may also be relevant. For example, the right to freedom of thought, conscience and religion and the right to freedom of assembly and association.[42] These also include, in the case of CSEA content, the right to privacy of victims of child sexual abuse and to the protection of their personal data.

e) The **potential impact** of the Technology Notice in reducing **the amount of terrorism or CSEA content**. 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 very substantial public interest that exists in measures that reduce its prevalence and dissemination online, including in relation to the prevention of crime and disorder, public safety, the protection of health or morals, and the protection of the rights and freedoms of others. As noted at d) above, in relation to CSEA content in particular, this can include the rights of children not to be subject to such abuse and harm, as well as the protection of their personal data.

A3.9 For a Technology Notice requiring the use of accredited technology, we expect to also consider the **terms and conditions** under which the service provider would be licensed to use the technology.

How we will approach our assessment of whether a technology is necessary and proportionate

A3.10 We have not sought in this guidance to set out the specific circumstances in which it might be necessary and proportionate to issue a Technology Notice, or the requirements that might be necessary and proportionate to impose in a particular case. This is because any decision to issue a Notice will be made on a case-by-case basis.

[41] 'Capacity' refers to (a) the financial resources of the service provider, and (b) the level of technical expertise which is available to the provider, or which it is reasonable to expect would be available to the service provider given its size and financial resources (section 236(1) of the Act).

[42] See Articles 9 and 11 of the ECHR.

A3.11 The specific requirements that are necessary and proportionate may vary between Technology Notices. We would expect to carefully consider these in each case but note that, in the case of a Notice requiring the use of **accredited technology**:

a) Ofcom would expect to carefully consider what kinds of content should be analysed by the accredited technology in each case. While we have the power to require the use of accredited technology on content communicated publicly (in the case of terrorism content), and on content communicated publicly and privately (in the case of CSEA content), we would not necessarily require the use of accredited technology on all such content. We might, for example, require the use of technology to deal with CSEA content on content communicated publicly only. Similarly, we might only require the use of technology on parts of a service, or in respect of certain functionalities.
b) We would also consider which specific accredited technologies might be appropriate in each case. By way of example, we recognise that, even if it is highly effective, a technology with a low throughput[43] may not be appropriate for a regulated user-to-user service where livestream content is being shared, because the technology takes too long to process content.
c) We would also consider the wider systems and processes that might be appropriate in each case. For example, the extent to which there should be human moderation of any content detected by the accredited technology.
d) Where appropriate, we would consider giving the service provider flexibility in any Technology Notice about which specific accredited technology it should use rather than specifying only one accredited technology.
e) We note that it may be appropriate in some cases to require the use of a combination of technologies (i.e., more than one accredited technology).

A3.12 We also note that it is more likely we would consider it necessary and proportionate to issue a Technology Notice to **develop or source technology** where a Notice to use accredited technology is not an option. This could be, for example, because there are no relevant accredited technologies or, where there are, it would not be technically feasible for any of those technologies to be used on the service and/or they would not be sufficient to address the specific harm(s). In such circumstances, we would expect to take into account the state of development of any technology which could be used to identify or prevent users' encountering CSEA content (even if not accredited), such as existing technological solutions.

A3.13 When reaching a view on whether to issue a Technology Notice and the requirements to be imposed on a service, we would expect to follow the process described in Sections A4 to A6 of this guidance. This would include obtaining a skilled person's report and giving the service provider the right to make representations on the requirements that we are considering imposing by means of a Warning Notice, both of which are required by the Act.

Compatibility testing

A3.14 We would also consider whether independent compatibility testing is appropriate to inform our view. This is notwithstanding that, in the case of a Technology Notice requiring the use of accredited technology, that technology would have already been accredited as meeting minimum standards of accuracy. In doing so, we would expect to have regard to:

[43] Throughput generally means how many units of information the technology can process in a given amount of time.

a) the extent to which there is independent and robust evidence available to Ofcom about the performance of the technology in question, and the relevance of that evidence to the specific use case in question; and
b) the extent to which use of the technology would result in solely automated decision making (or conversely, use of the technology would result in content being detected that is identical to content already determined by humans to be illegal content).

A3.15 The extent of any independent compatibility testing before issuing a Technology Notice would depend on the circumstances. For example, some limited initial testing may be appropriate to ascertain whether there may be suitable accredited technology for the use case in question, or if it would be more appropriate to explore exercising our power to issue a Notice to develop or source technology.

A3.16 Where Ofcom decides that more detailed compatibility testing is appropriate, this could include testing the technology against specific metrics using bespoke datasets representative of content the technology would expect to encounter on the service in question (e.g., illegal versus benign content, image, video, text etc.). This testing would measure the technology's capability at detecting and classifying the specific category(s) of relevant content we are concerned with. The technology may, for example, have been accredited to detect CSEA imagery generally, but we may be concerned about the prevalence of CSEA imagery of a specific age group on the service more specifically. In this case, compatibility testing done at this stage may focus on the performance of the technology at detecting CSEA content in a specific age group.

A3.17 Independent compatibility testing might also consider the performance of the technology against other metrics in the specific context of the service such as, for example, throughput. As discussed above, this metric could be important when considering whether it is necessary and proportionate to require the use of a particular accredited technology.

A3.18 The timing of any independent compatibility testing would depend on the circumstances. We expect any such testing would generally occur before we decide whether to issue a Warning Notice, although we might (in addition, or alternatively) conduct testing following any representations made by the service provider in response to a Warning Notice (see paragraphs A6.7 to A6.10).

A4. Initial assessment

Introduction

A4.1 Ofcom's OS Enforcement Guidance sets out the typical initial assessment process we will carry out when an issue comes to our attention.[44] We note that a Technology Notice is one of the regulatory tools available to us to resolve an issue.

A4.2 In this Section, we build on the OS Enforcement Guidance by explaining what might prompt us to initially consider exercising our Technology Notice functions (including how we might consider our power to issue a Technology Notice as part of the typical initial assessment process when we become aware of an issue which relates to relevant content), and the potential outcomes of an initial assessment.

How we may become aware of an issue

A4.3 We expect that the sources of information that might lead us to consider exercising our Technology Notice functions are likely to be the same as those which we use to identify and assess potential compliance issues, as set out in our OS Enforcement Guidance. These sources include, for example:

a) when an issue comes to light through our regular engagement with a service provider or industry;
b) routine monitoring of information provided to Ofcom, for example, our Consumer Contact Team or online safety complaints portal; or
c) information provided to us by other bodies (for example, other regulatory bodies, civil society organisations or enforcement agencies such as the NCA).

A4.4 It is important to note that the Online Safety regime is about service providers' safety systems and processes, not about regulating individual content found on such services. The presence of relevant content on a service does not necessarily mean that it would be necessary and proportionate to issue a Technology Notice. We would not therefore be likely to consider exercising our Technology Notice functions based on a complaint of a single piece of relevant content being present on a service. However, if we were to receive several complaints which indicate relevant content may be prevalent on, or disseminated by means of, a service this would be relevant to our assessment of whether it may be appropriate to exercise our Technology Notice functions.

Ofcom's initial assessment of the issue

The purpose of an initial assessment

A4.5 When Ofcom becomes aware of an issue, we will carry out an initial assessment to decide what action, if any, it may be appropriate to take. We have a variety of tools we can use to attempt to resolve the issue, including our power to issue a Technology Notice or open an investigation into a service provider's compliance with its obligations under the Act. The OS Enforcement Guidance explains in detail how we will carry out an initial assessment, and the

[44] See Section 4 of Ofcom's OS Enforcement Guidance.

range of statutory powers and non-statutory tools available to us. We highlight some of the key points below.

A4.6 Typically, the initial assessment will explore:

a) whether the available evidence merits taking action, having considered all relevant factors;
b) whether the issue is a priority for Ofcom; and
c) the most appropriate action to take in response to the issue.[45]

A4.7 We carry out an initial assessment on a case-by-case basis, having regard to our statutory duties and our priority framework (as set out in Section 3 of the OS Enforcement Guidance) to the extent relevant.[46]

A4.8 Where the issue concerns terrorism and/or CSEA content on a service, we may consider whether it would be appropriate to exercise our powers to issue a Technology Notice as part of our initial assessment. At this stage, we would expect to take into account, to the extent we are able to, the Specified Matters (and any other matters we may consider relevant) to consider whether it may be necessary and proportionate to issue a Notice.

A4.9 As part of our initial assessment, we may also engage with the service provider to give them an opportunity to comment on the issue(s), and to provide information to assist us in determining what action, if any, we should take. This may include exercising our statutory information gathering powers. We expect recipients to ensure that the information they provide to us is accurate, including where it has not been requested using our statutory information gathering powers.[47]

Potential outcomes of an initial assessment

A4.10 A senior member of Ofcom's staff with appropriate Board-delegated authority will make the decision about what the appropriate next steps will be, having regard to the available evidence. Typically, this will be the project supervisor who would also then oversee the project (see paragraph A5.3(a)).

A4.11 In line with our OS Enforcement Guidance, our initial assessment can result in Ofcom determining that the available evidence suggests it may be necessary and proportionate to issue a Technology Notice.[48] Where appropriate, we may also consider taking action using one or more of the other tools available to us alongside exercising our Technology Notice

[45] We will consider the level of detail and scope for the initial assessment as appropriate, bearing in mind the specific circumstances and the level of complexity of the issue.
[46] Our priority framework has been developed with all of our enforcement powers under the Act in mind and was not designed specifically for when Ofcom is considering whether it may be necessary and proportionate to issue a Technology Notice. Therefore, we would not expect all the priority factors to be relevant in those circumstances.
[47] See Section 4, paragraphs 4.8 to 4.14 of the OS Enforcement Guidance which provides more information on how we will engage with service providers during an initial assessment.
[48] See Section 4, paragraph 4.16 of Ofcom's OS Enforcement Guidance.

functions.[49] For example, where the issue relates to a compliance concern, we could also decide to open an investigation under the Act simultaneously.[50]

A4.12 We expect to inform the service provider of the outcome of an initial assessment and will typically do so via email (see paragraphs A5.2 to A5.4).

A4.13 If we decide that it may be necessary and proportionate to issue a Technology Notice, the typical process we will follow is set out in Sections A5 to A6 of this guidance. However, starting this process does not imply that we are satisfied that it would be necessary and proportionate to issue a Notice, nor that we will ultimately do so.

A4.14 Where we do not consider that issuing a Technology Notice may be necessary or proportionate as a result of our initial assessment (either because we have decided to use an alternative tool(s) available to us, or to take no further action), this would not stop us from reconsidering that as an option at a later stage. If we do, we will re-assess the issue taking into account the available evidence and all relevant factors.

[49] Section 4, paragraphs 4.15 to 4.29 of the OS Enforcement Guidance provide further detail on the potential outcomes of an initial assessment, which also include, for example, the use of one or more of our alternative compliance tools (such as commencing a period of compliance remediation); and applying to court for a business disruption order. We may also decide to take no further action, for example, where we are satisfied that the service provider has already taken steps to resolve the issue.

[50] Whilst we would typically announce that we have opened an investigation (see Section 5, paragraphs 5.14 to 5.21 of the OS Enforcement Guidance), we do not expect to announce that we have also decided it may be necessary and proportionate to issue a Technology Notice.

A5. Next steps and approach to information gathering

Introduction

A5.1 In this Section we explain what service providers can typically expect when we are considering issuing a Technology Notice, including how we will engage with the service provider, and our approach to information gathering during this stage.

Notifying the service provider

A5.2 As noted at paragraph A4.12, where we consider that it may be necessary and proportionate to issue a Technology Notice, we would expect to notify the service provider of our decision and will typically do so via email.

A5.3 We will usually provide the following information:

a) the **project team** (this will include the project lead, who will be the main point of contact at Ofcom, and the project supervisor, who will typically have been responsible for deciding appropriate next steps following our initial assessment and will be responsible for deciding whether to issue a Warning Notice);[51]
b) **our view that it may be necessary and proportionate** to issue a Technology Notice, including a summary of our concerns (for example, whether we are concerned about the prevalence or dissemination of terrorism or CSEA content, or both) and, where appropriate, any relevant information that has informed our view;
c) the **next steps** we intend to take, including an indication of the likely timescales; and
d) an explanation of how to raise a complaint and contact the **Procedural Officer**.[52]

A5.4 We may also ask the service provider to nominate a principal point of contact for communications about the issue.

Engaging with the service provider

A5.5 We will carefully consider, on a case-by-case basis, whether it would be necessary and proportionate to issue a Technology Notice. As such, we expect to engage with the service provider during the process, for example, before obtaining a skilled person's report or using any of our other information gathering powers.

A5.6 We will generally provide updates to the service provider on our progress, including when we expect to reach certain milestones. We will also provide updates where these change.

[51] Where we open an investigation at the same time, we expect the project team to be the same as the case team.
[52] If a service provider or any third party is dissatisfied with the way in which Ofcom is dealing with the matter, they should raise their concerns in writing with the project lead or project supervisor in the first instance. If their concern is not resolved, they may follow the process for contacting the Procedural Officer, which is outlined in Section 10 of the OS Enforcement Guidance.

A5.7 We may also meet with the service provider where we consider it appropriate for reasons of fairness and transparency. We will decide whether and when it is appropriate to do so depending on the circumstances.

Ofcom's information gathering powers

A5.8 We must obtain a skilled person's report before we can issue a Technology Notice. However, we may also use our other information gathering powers under the Act, either before obtaining a skilled person's report or concurrently. This could, for example, assist us in determining what skilled person(s) we should appoint or what specific issues they should address; obtain any information we need for the purposes of conducting any independent compatibility testing (see paragraphs A3.14 to A3.18); or confirm that information the service provider has provided during the initial assessment stage is accurate and complete.[53]

A5.9 Where we decide to use our information gathering powers, we will do so in line with our [draft] OS Information Powers Guidance.[54]

A5.10 Where appropriate, we may also gather further information from sources using methods other than our information gathering powers, such as public sources (e.g. openly available material on services' websites), engaging with services to obtain information informally or voluntarily, or information provided to us by other bodies (e.g. other regulators, law enforcement agencies).

Skilled person's reports

A5.11 The purpose of a skilled person's report in relation to our Technology Notice functions is:

a) to assist us in deciding whether to issue a Technology Notice; and
b) to advise about the requirements that might be imposed in such a Notice.[55]

A5.12 Where we obtain a skilled person's report for these purposes, we will have regard to Section A5 of our [draft] OS Information Powers Guidance, which sets out the process we will typically follow.[56] We note in particular:

a) In relation to the exercise of our Technology Notice functions, the skilled person must be appointed by Ofcom. Therefore, any references in our [draft] OS Information Powers Guidance regarding the service provider appointing a skilled person do not apply in these circumstances.
b) We will typically notify the service provider of the appointment via email and will specify the relevant matters to be explored in the report.[57]

---

[53] Our information gathering powers are set out in Chapter 4 of Part 7 of the Act. These include our power to issue a notice requiring information already held by the recipient of the notice or requiring the recipient to obtain or generate information. Our approach to information gathering may differ if we open an investigation at the same time as considering whether it is necessary and proportionate to issue a Technology Notice. If appropriate, we may decide to appoint a skilled person under section 104 of the Act to prepare a combined report about matters relevant to both our investigation and our consideration of whether to issue a Notice.
[54] Ofcom, [draft] OS Information Powers Guidance.
[55] Section 122(2) of the Act.
[56] See section 104(6), which sets out what a skilled person is for the purposes of section 104, see also paragraph A5.5 of Ofcom's [draft] OS Information Powers Guidance.
[57] Section 104(4) of the Act. See also paragraphs A3.50 to A3.54 of Ofcom's [draft] OS Information Powers Guidance for information on how we will serve information notices.

c) The provider of the service is liable for the payment, directly to the skilled person, of the skilled person's remuneration and expenses relating to the preparation of the report.[58]

A5.13 The relevant matters we will ask a skilled person to advise on will depend on the specific circumstances and issue that we are considering, including the information that Ofcom already has available to it. For example, we may request that the skilled person's report explains the service provider's existing systems and processes to identify relevant content, and how (and where) accredited technology could be implemented alongside this, or provide information on the prevalence of such content on the service. We may also request that the skilled person conduct separate testing, or suggests any testing that Ofcom may undertake when we are considering whether to issue a Technology Notice.

Duties of the service provider

A5.14 The Act places duties on service providers to comply with the requirements imposed on them in the exercise of our information powers. Specifically, in relation to skilled person's reports, this includes a duty to give the skilled person all such assistance as they may reasonably require in preparing the report.[59]

A5.15 The requirements that may be imposed when exercising our information gathering powers are enforceable by Ofcom, and failure to comply with them can result in significant consequences, including Ofcom taking enforcement action under the Act. Enforcement action may result in a decision to impose a financial penalty and/or requirements to take specified steps to come into compliance and/or remedy the non-compliance.[60]

[58] If the service provider fails to make payment, the amount due can be recovered by order of court. See section 104(8) to (12) of the Act.
[59] See Section 104(7) of the Act and Section A8 of Ofcom's [draft] OS Information Powers Guidance.
[60] See Section 5, paragraphs 5.40 to 5.44 of the OS Enforcement Guidance.

A6. Deciding whether to issue a Technology Notice

Introduction

A6.1 This Section explains the stages of our process from deciding whether to issue a Warning Notice, including the service provider's right to make representations, to deciding whether to issue a Technology Notice.

Decision to issue a Warning Notice

A6.2 Once we have considered the contents of the skilled person's report, and any other relevant evidence (including the results of any compatibility testing where relevant (see paragraphs A3.14 to A3.18), we will consider whether it is necessary and proportionate to issue a Technology Notice to the service provider in question. If we provisionally consider that it is, we will first issue a Warning Notice, which will explain why we are minded to issue a Technology Notice and the requirements we are considering imposing.

A6.3 While we will consider the Specified Matters when deciding whether to issue a Warning Notice, a decision to issue one does not necessarily mean that we will go on to issue a Technology Notice. This decision will only be made after the service provider has had the opportunity to make representations in response to the Warning Notice (see below).

A6.4 We will typically send the Warning Notice to the service provider via email.[61]

Information contained in the Warning Notice

A6.5 The Warning Notice will contain the information specified in the Act, and other information we consider appropriate.[62] This will include:

a) The reasons why we provisionally consider that it is necessary and proportionate to issue a Technology Notice, including a summary of the skilled person's report, together with any other evidence on which we have relied to reach our provisional conclusions.
b) The requirements we are considering imposing, which would include:

i) in the case of a Warning Notice relating to the **development or sourcing** of technology, the specific steps that we consider the service provider should be required to take. We expect one of those steps would be that any technology ultimately developed or sourced by the service provider is tested to understand whether it meets the minimum standards of accuracy,[63] although this does not

[61] Section 208 of the Act prescribes the ways in which Ofcom can serve notices. See also section 123(4) of the Act in relation to how Ofcom may issue a Warning Notice in relation to both the user-to-user part, and the search engine part of a combined service. See also footnote 4.
[62] See section 123 of the Act. The information Ofcom is required to include in a Warning Notice relating to a) the use accredited technology, is set out in section 123(2); and b) the development or sourcing of technology, is outlined in section 123(3) of the Act.
[63] This is because technology that is required to be developed or sourced under the Act should meet the minimum standards of accuracy published by the Secretary of State.

mean that we would require the service provider to allow the technology it has developed or sourced to be used by another service provider in a Notice; and

ii) in the case of a Warning Notice relating to the use of **accredited technology**, the technology (or combination of technologies) we consider should be used, and the manner in which it should be implemented.[64] For example, on which specific kind(s) of content or parts of the service it should be implemented, where relevant.[65] The requirements could also, for example:

- relate to the wider systems and processes used by the service provider, such as the use of human moderators and/or the operation of an effective complaints procedure (where relevant); and
- set out any proportionate changes to the service's infrastructure that may be needed in order to effectively implement the technology or a requirement (where a service provider is already using accredited technology) to do so more effectively.

c) The period for which we are considering imposing the requirements and timescales for compliance and/or steps to be taken (see paragraphs A6.18 to A6.20 below).

A6.6 It will also give the service provider an opportunity to make representations (with any supporting evidence) about the matters contained in the Warning Notice and specify the period within which they can make representations, and the process for doing so.

Consideration of representations on the warning notice

A6.7 Ofcom will not issue a Technology Notice until after the specified period for representations has passed.[66]

A6.8 Typically, Ofcom will give a period of at least **20 working days** to make written representations in response to the Warning Notice. The period will however depend on the individual circumstances, and we recognise that there may be circumstances where service providers may require a longer period to provide representations. There may also be exceptional circumstances where an expedited process is appropriate.

A6.9 If the service provider makes representations in response to the Warning Notice (in the time specified for response), then Ofcom will consider these representations in full before deciding whether to issue the Technology Notice.[67]

A6.10 The service provider is under no obligation to provide representations. If no representations are received (or the service provider notifies Ofcom that it does not wish to make any) by the time the period for representations has expired, and no further information has come to

[64] If we are proposing to give the service provider flexibility to choose between different accredited technologies in order to comply with the Notice (see paragraph A3.11(d)) this would be made clear in the Warning Notice.
[65] See paragraph A3.11(a).
[66] Section 123(5) of the Act.
[67] It is possible, as discussed in Section A3, that Ofcom may also consider it appropriate for independent compatibility testing to be conducted following the receipt of representations (and before Ofcom decides whether to issue a Technology Notice).

light since the Warning Notice was issued, Ofcom will then proceed to make a decision about whether it is necessary and proportionate to issue the Technology Notice.

Decision to issue a Technology Notice

A6.11 Ofcom will nominate a final decision maker who will decide, taking account of all relevant evidence and written representations, whether it is necessary and proportionate to issue a Technology Notice. The final decision maker will be a senior member of Ofcom's staff with appropriate Board-delegated authority.

A6.12 In reaching that decision, we would expect to take into account the matters discussed in Section A3, and any decision will be taken by Ofcom on a case-by-case basis.

A6.13 We may decide not to issue a Technology Notice at this stage, and may decide that no further action is required, or that it is appropriate to use other tools available to Ofcom to address the issue.[68]

A6.14 Where we are satisfied that it is necessary and proportionate to issue a Technology Notice, we will typically issue the notice in electronic form, via email.[69]

Information contained in the Technology Notice

A6.15 The Technology Notice will contain the information specified in the Act, and any other information we consider appropriate.[70] In line with the Warning Notice, this will include:

a) the reasons why we consider it necessary and proportionate to issue a Notice, including a summary of the evidence on which we have relied;
b) the requirements we have decided to impose in the Notice; and
c) the period for which we are imposing the requirements and/or within which any steps must be taken (see paragraphs A6.18 to A6.20 below).

A6.16 While it will contain the same type of information as the Warning Notice (albeit setting out Ofcom's final decision), it may be substantially different from the Warning Notice, particularly in light of representations made by the provider.

A6.17 The Technology Notice will also outline when Ofcom intends to review the service provider's compliance with the Notice; the service provider's right of appeal under the Act; and the consequences of non-compliance, including the further kinds of enforcement action Ofcom may take (see Section A7).

Timescales for compliance

A6.18 Any period(s) we specify in a Technology Notice will be in line with the Act (see paragraphs A2.27 to A2.29) and will be assessed on a case-by-case basis, taking into account all relevant information and evidence available and those factors that appear to us to be relevant in the circumstances.

A6.19 In relation to a Technology Notice requiring the use of accredited technology, we note we must specify a reasonable period for the service provider to take any action required to comply with the Notice; for example, to purchase the accredited technology or make any

[68] See paragraphs A4.10 to A4.14.
[69] See footnote 61.
[70] See sections 125(6) and (8) of the Act (as appropriate).

proportionate changes to the design or operation of the service which are necessary for the technology to be used effectively.

A6.20 For a Technology Notice relating to developing or sourcing technology, we will specify a reasonable period within which the service provider must take each step set out in the Notice, taking into account, in particular, the size and capacity of the provider, and the state of development of technology capable of achieving the purpose described in the Notice.[71]

[71] Section 125(9) of the Act.

A7. Next steps after issuing a Technology Notice

Introduction

A7.1 This Section explains the next steps following a Technology Notice being issued to a service provider, including when Ofcom would typically review the service provider's compliance with the Notice and the consequences of non-compliance.

Reviewing compliance with a Technology Notice

A7.2 Where Ofcom has issued a Technology Notice to a service provider, and it has not been revoked (see from paragraph A7.15 below), we will carry out a review of the service provider's compliance with the Notice.

A7.3 We will generally notify the service provider before commencing a review and will provide contact details of the project team and our proposed next steps. The process and length of the review will depend on the circumstances; however, we expect to also engage with the service provider during the review to ensure that we gather all relevant information to assist us in the process, and will aim to update them where appropriate, and keep them informed of important milestones.

A7.4 We may use one or more of our information gathering powers to obtain the information we consider would be relevant in assisting our review.[72]

A7.5 For a Technology Notice requiring the use of **accredited technology**, we must carry out a review before the Notice expires and would typically expect to begin that review no earlier than six months before that date. We will, as part of our review, consider the extent to which the technology specified in the Notice has been used and the effectiveness of its use.[73]

A7.6 We would expect to also engage with the service provider at appropriate intervals during the period of the Technology Notice requiring the use of **accredited technology** being in effect, for example, to confirm they have taken any action needed to comply with the Notice after the deadline for implementation in the Notice has passed.

A7.7 For a Technology Notice requiring the **development or sourcing of technology**, we must review the service provider's compliance with the Notice before the last date by which any step specified in the Notice is required to be taken. It is therefore likely that we will conduct a review on more than one occasion. The timing and frequency of the review and what we will consider during the review will vary on a case-by-case basis depending on the steps specified in the Notice. The fact that the service provider has not been able to develop or source technology which serves the purpose specified by the Notice and meets the minimum standards of accuracy does not necessarily mean that it has failed to comply with the Notice; we may be satisfied that it has nevertheless used its best endeavours.

[72] If appropriate, we may also obtain a skilled person's report.
[73] Section 126(5) of the Act.

A7.8 Following our review, a senior member of Ofcom's staff with appropriate Board-delegated authority will decide the appropriate next steps, which may include:

a) that we are satisfied that the requirements, or specified step(s), in the Technology Notice have been complied with;
b) that we are satisfied that the requirements, or specified step(s), in the Technology Notice have **not** been complied with, in which case we might issue a notice requiring the payment of a penalty (a 'penalty notice') (see paragraphs A7.22 to A7.24) or apply to court for a business disruption order (see paragraphs A7.25 to A7.27);
c) that we vary or revoke the Notice (see paragraphs A7.15 to A7.19);
d) that it is necessary and proportionate to issue a further Notice (see paragraphs A7.11 to A7.14).

A7.9 The next steps set out above are not necessarily mutually exclusive. For example, Ofcom may issue a penalty notice where it is satisfied that the requirements in a Technology Notice have not been complied with, while also issuing a further Notice.

A7.10 We will notify the service provider of the outcome of our review via email. We may also arrange a meeting to discuss the outcome.

Further Notices

A7.11 We may issue a further Technology Notice if we consider it necessary and proportionate to do so and following consultation with the service provider.[74] Such a Notice may impose different requirements from those imposed under the earlier Notice.

A7.12 Where this is the case, we will take into account all the Specified Matters, and any other matters we consider to be relevant (see Section A3).

A7.13 Where we decide to issue a further Technology Notice, we are not required to obtain a further skilled person's report or issue a further Warning Notice. However, we may do so if we consider it appropriate in the circumstances; for example, where we are intending to impose substantially different requirements from those contained in the earlier Notice. Where we decide to issue a Warning Notice, we would give the service provider the opportunity to make representations.

A7.14 Where we issue a further Notice, we will carry out a review of the service provider's compliance with the requirements in that further Notice as outlined above.

Revoking or varying a Technology Notice

A7.15 Ofcom may revoke a Technology Notice by notifying the service provider to that effect.[75] This may be, for example, where we have reasonable grounds for believing that the service provider is failing to comply with it or where we consider that it is no longer necessary and proportionate for the Notice to remain in effect.

[74] See sections 126(6) to 126(9).
[75] Section 125(11) and 126(2) of the Act.

A7.16 Where we decide to revoke a Technology Notice, we may decide that it is necessary and proportionate to issue a further Notice, taking into account the Specified Matters (see paragraphs A7.11 to A7.14).[76]

A7.17 We may also decide to vary a Notice by notifying the service provider to that effect.[77] This may be, for example, where new evidence or information leads us to consider making material changes to it.

A7.18 We will generally engage with the service provider where we are considering revoking or varying a Technology Notice and will give the service provider an opportunity to provide representations on our proposal(s).

A7.19 Where we decide that it is appropriate to vary or revoke a Technology Notice, we will typically notify the service provider of our decision via email.

Consequences of non-compliance with a Technology Notice

A7.20 It is important that service providers comply with the requirements imposed by Ofcom in a Technology Notice. Failure to comply with such requirements may carry significant consequences including, as noted above, a decision by Ofcom that it is necessary and proportionate to issue a further Notice (including a further Notice which imposes different requirements from those included in the earlier Notice).

A7.21 It can also result in Ofcom using its enforcement powers under the Act, which could include issuing a penalty notice and/or applying to court for a business disruption order.

Penalty notices

A7.22 Ofcom may issue a penalty notice where it is satisfied that a service provider has failed or is failing to comply with the requirements in a Technology Notice.[78]

A7.23 Where Ofcom proposes to issue a penalty notice, it will do so in line with the Act, and will follow the guidance set out in Section 6 of the OS Enforcement Guidance in relation to provisional notices of contravention and confirmation decisions to the extent relevant.[79]

A7.24 Where we decide to impose a penalty notice, we may impose a financial penalty of up to 10% of qualifying worldwide revenue or £18 million (whichever is the greater).[80] Any penalty that we impose will be set in accordance with our Penalty Guidelines.[81] In determining the amount of any penalty, Ofcom will consider all the circumstances of the case, and will take into account the potentially relevant factors set out in the Penalty Guidelines.

[76] Section 126(3) of the Act.
[77] Section 125(11) and 126(2) of the Act.
[78] See section 140 of the Act.
[79] See in particular, Section 6, paragraph 6.57 of the OS Enforcement Guidance. Before Ofcom can issue a penalty, it will first issue a notice setting out its intention to impose a penalty and provide an opportunity for the service provider to make representations about the matters contained in that notice.
[80] See Schedule 13 of the Act.
[81] See Ofcom's, 2017 Penalty Guidelines as amended.

Business disruption orders

A7.25 Ofcom may apply for a business disruption order where a provider of a Part 3 service has failed to comply with a Technology Notice and that failure is continuing.[82]

A7.26 Business disruption measures are orders made by a Court on an application from Ofcom.[83] They apply to third parties which are in a position to take action to disrupt the provision of the regulated service and thereby reduce the risk of harm to UK citizens and consumers. Business disruption measures are a significant regulatory intervention and include:

a) a service restriction order; or interim service restriction order;[84] and
b) an access restriction order; or an interim access restriction order.[85]

A7.27 Where Ofcom considers applying for a business disruption order, it will do so in line with the Act, and will follow the guidance set out in Section 9 of our OS Enforcement Guidance.

[82] Section 144(4) and section 146(1)(a), See also sections 145(4) and section 147(1)(a) of the Act, which provides that Ofcom may apply for an interim service or access restriction order where it is likely that the provider of the Part 3 service is failing to comply with a Technology Notice and the level of risk of harm to individuals in the United Kingdom relating to the likely failure, and the nature and severity of that harm, are such that it would not be appropriate to wait to establish the failure before applying for the order.
[83] See sections 144 to 148 of the Act in relation to Ofcom's power to apply to court for business disruption measures.
[84] A service restriction order is an order applying to one or more providers of ancillary services that facilitates the provision of the regulated service (such as payment processing services or ad servers). See Section 9, paragraphs 9.6 to 9.7 of the OS Enforcement Guidance.
[85] An access restriction order is an order applying to one or more providers of facilities which enable access to a service (such as internet access services or an App store). See Section 9, paragraphs 9.8 to 9.9 of the OS Enforcement Guidance.

A8. Disclosure of information and publication

Introduction

A8.1 In this Section, we outline how we expect to approach the disclosure of information and publication about the exercise of our Technology Notice functions. Any information that we disclose or publish will be in line with the [draft] Information Powers Guidance and the OS Enforcement Guidance.[86]

Disclosing information to third parties

A8.2 We are likely to gather information relating to a particular business using our information gathering powers (including by means of the skilled person's report) when exercising our Technology Notice functions. When we do so, section 393 of the Communications Act will apply. This prohibits Ofcom from disclosing that information without the consent of the person carrying on that business, unless this is permitted for specific, defined purposes.[87]

A8.3 One of the purposes for which we are able to disclose information about a particular business (including confidential information) is where this is for the purpose of facilitating the exercise of our online safety functions, including our Technology Notice functions. This would include, for example, where we disclose information to a skilled person for the purposes of their preparation of a skilled person's report. Where we do so, we will carefully consider whether the information we are proposing to share with the skilled person is relevant to the purpose of their report.

Publishing details about decisions

A8.4 Ofcom is required to have regard to the principle under which regulatory activities should be transparent and accountable. We therefore generally publish information about significant actions we take and would expect to publish updates at important milestones, for example, where we issue a Warning Notice or a Technology Notice, or where we issue a further Notice, or revoke a Notice.

A8.5 Where we issue a Warning Notice, we may announce this on our website. Where we do so, we expect to provide details of the service provider to whom the Warning Notice relates, publish a summary of our proposed requirements and a summary of our reasons for issuing the Warning Notice.

A8.6 Where we issue a Technology Notice, or a further Notice, we will generally announce this on our website and provide details of the service provider to whom we have issued the Notice, a summary of the requirements we have imposed, and a summary of our reasons. When considering how much information to publish about the Notice, we will be mindful of the

[86] See Section A3 of Ofcom's [draft] OS Information Powers Guidance.

[87] This prohibition would also apply to any skilled person that has gathered information relating to a particular business for the purpose of preparing their report for Ofcom under section 122 of the Act.

need to disclose enough information to enable persons with a sufficient interest to exercise their right of appeal under section 168 of the Act.

A8.7 While we do not generally expect to publish Technology Notices in full, we will take decisions on a case-by-case basis and may do so in appropriate circumstances; for example, where it is in the interests of citizens and consumers. Where we do decide to publish a Notice, we will not publish information we consider to be confidential and will create a non-confidential version of it, which we will share with the service provider prior to publication and give them the opportunity to provide representations on confidentiality (see from paragraph A8.16 below).

A8.8 Where we have issued a penalty notice for non-compliance of a Technology Notice, we will publish details of our enforcement action in line with Sections 149 and 150 of the Act.[88]

A8.9 Where we have obtained an order for business disruption measures from the Court, we will publish a statement to this effect on our website.[89]

A8.10 We do not agree the text of website updates or media releases with service providers. Where appropriate, we will inform the service provider no more than one working day before publication on Ofcom's website that we will be doing so and provide it with a copy of the intended text of the update.

A8.11 Where we consider an announcement to be potentially market sensitive, we will generally inform the service provider after markets have closed, with publication at 7.00am on Ofcom's website and via the Regulatory News Service, just before markets open. Where the service provider is a listed company in other jurisdictions, we will, where possible, seek to avoid publication during stock exchange hours in those jurisdictions.

Ofcom's Annual Report

A8.12 The Act requires Ofcom to produce an annual report about the exercise of its Technology Notice functions and technology which meets (or is in the process of development so as to meet) minimum standards of accuracy for the purposes of these functions.[90]

A8.13 Examples of the matters we would generally expect to address in our annual report include, but are not limited to:

- a list of those technologies that are, at the date of the annual report, accredited as meeting the minimum standards of accuracy approved and published by the Secretary of State;
- a summary of any technology being developed to meet those minimum standards of accuracy; and
- an update on how many Technology Notices we have issued in the period to which the annual report relates, together with a summary of the requirements we have imposed.

A8.14 While the general restriction in section 393 of the Communications Act does not apply where Ofcom is publishing a report under the Act, we must have regard to the need to exclude confidential information from publication, so far as is practicable. Confidential

[88] See Section 6, paragraphs 6.59 to 6.68 of the OS Enforcement Guidance.
[89] See Section 9, paragraph 9.27 of the OS Enforcement Guidance.
[90] Section 128(1)(a) and 128(1)(b) of the Act.

information means information that relates to the affairs of a body or private affairs of an individual, the publication of which would or might seriously and prejudicially affect the interests of that body or individual.

A8.15 In addition, we would not expect to include any information about any Warning Notices and/or final Technology Notices referred to in our annual report that we have not published in line with paragraphs A8.4 to A8.11 above.

Confidentiality

A8.16 Ofcom is mindful of the importance of protecting confidential information and will generally redact such information or withhold it from disclosures that we make for the purposes of exercising our functions. However, it is occasionally necessary to disclose confidential information to facilitate the performance of our functions (such as, for example, with a skilled person).

A8.17 As noted above, Ofcom may publish information about Technology Notices. If Ofcom is proposing to publish information which a party considers confidential, we will take reasonable steps to inform that party and give it a reasonable opportunity to make representations on our proposal, before making a final decision on whether to disclose. This decision will be made by the project team and/or the project supervisor and will be communicated to the party concerned in advance of the disclosure being made.

A8.18 Where parties consider information is confidential, they should explain their reasons for this. We do not accept unsubstantiated blanket claims of confidentiality and it is for Ofcom to decide whether the information is confidential. Parties may escalate concerns relating to confidentiality to the Procedural Officer (in accordance with Section 10 of the OS Enforcement Guidance). We would expect to delay disclosing information until the Procedural Officer has reached their decision. If we intend to disclose the information after taking these steps, we will inform the party concerned in advance.