ONLINE SAFETY BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the parts and clauses of the Online Safety Bill as published in draft on 12 May 2021 (Bill CP 405).

- These Explanatory Notes have been provided by the Department for Digital, Media, Culture and Sport and the Home Office in order to assist the reader of the Bill. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might be best read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

Overview of the Bill 4

Policy background 5
- Interim Codes of Practice 6
- Government Report on Transparency Reporting 6

Legal background 7

Territorial extent and application 9

Commentary on provisions of Bill 10

Part 1: Overview and key definitions 11

Part 2: Providers of Regulated Services: Duties of Care 14
- Chapter 1: Introduction 14
- Chapter 2: Providers of user-to-user services: Duties of care 14
- Chapter 3: Providers of search services: duties of care 22
- Chapter 4: Assessment about access by children 27
- Chapter 5: Codes of practice 29
- Chapter 6: Interpretation of Part 2 36

Part 3: Other Duties of Service Providers 42
- Chapter 1: Transparency Reports 43
- Chapter 2: Fees 44

Part 4: OFCOM'S Powers and Duties in Relation to Regulated Services 49
- Chapter 1: General Duties 49
- Chapter 2: Register of Categories of Services 50
- Chapter 3: Risk assessments 56
- Chapter 4: Use of technology in relation to terrorism content and child sexual exploitation and abuse content 57
- Chapter 5: Information 61
- Chapter 6: Enforcement Powers 71
- Chapter 7: Committees, research and reports 87
- Chapter 8: Media literacy 90

Part 5: Appeals and Super-complaints 92
- Chapter 1: Appeals 92
- Chapter 2: Super-complaints 93

Part 6: Secretary of State's Functions in Relation to Regulated Services 96

Part 7: General and Final Provisions 100

Financial implications of the Bill 114

Compatibility with the European Convention on Human Rights 115

Related documents 116

Annex A – Glossary 117

Annex B - Territorial extent and application in the United Kingdom 119

Subject matter and legislative competence of devolved legislatures 121

Overview of the Bill

1. The Online Safety Bill establishes a new regulatory regime to address illegal and harmful content online, with the aim of preventing harm to individuals in the United Kingdom. It imposes duties of care in relation to illegal content and content that is harmful to children on providers of internet services which allow users to upload and share user-generated content ("user-to-user services") and on providers of search engines which enable users to search multiple websites and databases ("search services").

2. The Bill also imposes duties on such providers in relation to the protection of users' rights to freedom of expression and privacy. Providers of user-to-user services which meet specified thresholds ("Category 1 services") are subject to additional duties in relation to content that is harmful to adults, content of democratic importance and journalistic content.

3. The Bill confers powers on the Office of Communications (OFCOM) to oversee and enforce the new regulatory regime (including dedicated powers in relation to terrorism content and child sexual exploitation and abuse (CSEA) content), and requires OFCOM to prepare codes of practice to assist providers in complying with their duties of care. The Bill also expands OFCOM's existing duties in relation to promoting the media literacy of members of the public.

Policy background

4. With the increasing use of the internet has come an increasing awareness that online content can cause serious harm to users and other individuals in the United Kingdom. The prevalence of the most serious illegal content and activity online is unacceptable, and it threatens the United Kingdom's national security and the physical safety of children. There were more than 69 million images and videos related to child sexual exploitation and abuse referred by US technology companies to the National Center for Missing and Exploited Children in 2019, an increase of more than 50% on the previous year.

5. Alongside illegal content and activity, there are increasing levels of public concern about online content and activity which is lawful but potentially harmful. This type of activity can range from online bullying and abuse, to advocacy of self-harm, to spreading disinformation and misinformation. Whilst this behaviour may fall short of amounting to a criminal offence, it can have corrosive and damaging effects, creating toxic online environments and negatively impacting users' ability to express themselves online.

6. The Bill is intended to make the services it regulates safer by placing responsibilities on the providers of those services in relation to content that is illegal or which, although legal, is harmful to children or adults.

7. The Online Harms White Paper, published in April 2019, set out the intention to improve protections for users online through the introduction of a new duty of care on companies and an independent regulator responsible for overseeing this framework. It proposed that this regulation follow a proportionate and risk-based approach, and that the duty of care be designed to ensure that all companies have appropriate systems and processes in place to address harmful content and improve the safety of their users.

8. A public consultation on the White Paper proposals ran from 8 April 2019 to 1 July 2019. It received over 2,400 responses ranging from companies in the technology industry including large tech giants and small and medium sized enterprises, academics, think tanks, children's charities, rights groups, publishers, governmental organisations and individuals.

9. In February 2020, the government published an initial response to the consultation, providing an in-depth breakdown of the responses to each of the 18 consultation questions asked in relation to the White Paper proposals. The response also set out the government's direction of travel in a number of key areas, including:

    a. How the new regulatory framework would ensure protections for users' rights by including safeguards in the legislation;

    b. The differentiated approach to illegal and legal material;

    c. How the new requirements would be proportionate and risk-based, including clarifying who would not be captured by the proposed scope;

    d. A commitment to delivering a higher level of protection for children; and

e. That the government was minded to appoint OFCOM as the new regulator.

10. In December 2020, the full government response to the consultation was published, outlining the final policy position for the online safety regulatory framework, and the government's intention to enshrine it in law through the Online Safety Bill. The response was split into seven parts:

    a. Part 1 stated that the regulatory framework would apply to companies whose services host user-generated content or facilitate interaction between users, one or more of whom is based in the UK, as well as to search engines.

    b. Part 2 outlined that the legislation would set out a general definition of the harmful content and activity covered by the duty of care. It also set out how all companies in scope would be required to understand the risk of harm to individuals on their services, and to put in place appropriate systems and processes to improve user safety and monitor their effectiveness.

    c. Part 3 confirmed that OFCOM would be appointed as the regulator, and outlined its regulatory functions and funding.

    d. Part 4 explained the proposed functions of the regulator, including its duty to set out codes of practice, enforcement powers, and user redress mechanisms.

    e. Part 5 outlined the role of technology, education, and awareness in tackling online harms.

    f. Part 6 explained how the new regulatory framework would fit into the wider digital landscape, including as part of the government's Digital Strategy.

    g. Part 7 provided the next steps for the regime, including the expected timings for the Online Safety Bill.

Interim Codes of Practice

11. The government published two interim codes of practice covering terrorist content and child sexual exploitation and abuse (CSEA) content online alongside the full government response. These interim codes set out the voluntary action the government expects providers to take to tackle the most serious categories of harmful content online before the regulator is established.

Government Report on Transparency Reporting

12. The first government report on transparency reporting in relation to online harms was published alongside the full government response. This presented the recommendations of the multi-stakeholder transparency working group, set up in October 2019, about how the transparency framework could work in practice within the new online harms regulatory framework.

Legal background

13. The Online Safety Bill repeals the following existing legislative provisions which relate to the regulation of internet services:

    a. Part 3 of the Digital Economy Act 2017 (online pornography);

    b. Section 103 of the Digital Economy Act 2017 (code of practice for providers of online social media platforms); and

    c. Part 4B of the Communications Act 2003 (video-sharing platform services) and Part 4 of the Audiovisual Media Services Regulations 2020 (S.I. 2020/1062) (which inserts Part 4B into the Communications Act 2003).

14. OFCOM was established by the Office of Communications Act 2002. The Bill amends OFCOM's general duties, as set out in section 3 of the Communications Act 2003, to extend them in relation to online safety matters, and substitutes revised provisions for OFCOM's existing duty to promote media literacy in section 11 of that Act.

15. Prior to the UK's exit from the European Union, the legal framework for the regulation of online services was primarily set out in the EU e-Commerce Directive (eCD)[1]. The eCD detailed the rules for online service providers in respect of transparency and information requirements, rules for cooperation between member states, and, most importantly for the Bill's purposes, a framework limiting the liability of online intermediaries for the content they host on their services.

16. The eCD prevented member states from imposing liability on service providers who provide a service that 'consists of the storage of information provided by the recipient of the service' for content created by users, so long as '*the provider does not have actual knowledge of illegal activity or information and ... is not aware of facts or circumstances from which the illegal activity or information is apparent'.* This limitation was contingent on the host, upon gaining knowledge of such content, removing it expeditiously. Article 15 of the eCD also contained a prohibition on the imposition of requirements on service providers to generally monitor content they transmit or store, or to actively seek facts or circumstances indicating illegal activity.

17. The status of the eCD following the UK's exit from the EU is governed by the European Union Withdrawal Act 2018 (EUWA), which contains some provision for the continued operation of EU law. Section 5 of the EUWA holds that the supremacy of EU law ceased following the end of the transition period. This means there is no longer a legal obligation on the UK to legislate in line with the provisions of the eCD following the end of the transition period on 31 December 2020.

18. The Communications Act 2003 governs communications more generally, with Part 1 of the Act setting out OFCOM's functions in relation to communications.

[1] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

19. Other related legislation includes the Digital Economy Act 2017, section 103 of which obliges the Secretary of State to issue a code of practice for providers of online social media platforms. Part 3 of the Digital Economy Act put forward a statutory requirement for all commercial pornographic websites to prevent children's access. The Act received Royal Assent in April 2017 but Part 3 was not fully commenced. The government announced in October 2019 that it would not commence Part 3 of the 2017 Act, and would instead repeal Part 3 and deliver its objectives through the online harms regulatory framework.

20. The Audiovisual Media Services Regulations 2020 transposed the EU's revised Audiovisual Media Services Directive (AVMSD)[2], which was designed to provide minimum standards and market access for cross border broadcasters, including Video on Demand services throughout the European Economic Area. The AVMSD also introduced new measures to protect children from content provided by video-sharing platforms which 'may impair their physical, mental or moral development'. This included platforms that provide user-generated video to the public over which they have no editorial control for commercial purposes.

[2] Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services.

Territorial extent and application

21. Clause 139 sets out the territorial extent of the Online Safety Bill. The extent of a Bill can be different from its application. Application is about where a Bill produces a practical effect rather than where it forms part of the law. The Online Safety Bill extends and applies to the whole of the UK. In addition, repeals and amendments made by the Bill have the same territorial extent as the legislation that they are repealing or amending.

22. The Bill also applies to providers of regulated services (as defined in clause 3) which are based outside the UK. Extraterritorial application is necessary in order to fulfil the Bill's aim of protecting UK users online. Clauses 127 and 128 make provision in relation to the extraterritorial application of the Bill.

23. Internet law and regulation is a reserved policy area. The matters to which the provisions of the Bill relate are not within the legislative competence of the devolved administrations.

24. The Bill contains criminal offences in relation to failures to comply with information requests from OFCOM. These offences apply and extend to the whole of the United Kingdom. These offences also apply where the entity or individual provides a regulated service under the Bill from overseas (and commits the offence overseas).

25. See the table in Annex B for a summary of the position regarding territorial extent and application in the United Kingdom.

Commentary on provisions of Bill

26. The Bill is divided into seven parts:

    a. **Part 1** contains definitions of the services to which the Bill applies.

    b. **Part 2** sets out the duties of care that apply to providers of user-to-user and search services. These are duties to undertake risk assessments, and also duties with regards to content on their services that is illegal, harmful to children and harmful to adults.

    c. **Part 3** sets out further obligations on services in relation to transparency reporting and the payment of fees.

    d. **Part 4** sets out OFCOM's powers and duties as the online safety regulator. There are specific provisions on OFCOM's duties to carry out risk assessments and to maintain a register of categories of services. Part 4 also establishes OFCOM's functions and powers with respect to the use of technology in relation to terrorism content and child sexual exploitation and abuse (CSEA) content, information-gathering, enforcement, research, and media literacy.

    e. **Part 5** provides for the grounds and avenues for appeals against decisions by OFCOM, and for designated bodies to make super-complaints to the regulator.

    f. **Part 6** provides for the powers of the Secretary of State to issue a statement of strategic priorities and guidance to OFCOM, and to review the regulatory framework established by the Bill.

    g. **Part 7** contains miscellaneous and general provisions. In particular, it defines key concepts such as providers of regulated services, users, and internet services.

Part 1: Overview and key definitions

Clause 1: Overview of Act

27. The first clause sets out the purpose of the various parts of the Bill.

Clause 2: Meaning of "user-to-user service" and "search service"

28. This clause provides definitions for the terms "user-to-user service" and "search service". These are the two primary types of services that may be subject to regulatory duties.

29. Subsection (1) defines a user-to-user service as an internet service (see clause 133) which allows users to generate, upload or share content which may be encountered by others on that service. Subsection (2) makes clear that this includes content which may be encountered by others through a functionality on the service (such as a functionality to send a direct message). Subsection (3) states that a service with user-generated content is a user-to-user service regardless of the proportion of user-generated content on that service.

30. Subsection (4) cross-references the definitions of "content" and "encounter" in clause 137 of the Bill. For the purposes of the Bill "content" means anything communicated by means of an internet service (as defined in clause 133), whether publicly or privately, and "encounter" means read, view, hear or otherwise experience.

31. Subsection (5) sets out that a search service means an internet service that is, or includes, a search engine (as defined in clause 134) and which is not a user-to-user service.

32. Subsection (6) allows that any dissociable part of a user-to-user or search service will be exempt from regulatory duties if that dissociable part meets the conditions to benefit from the internal business exemption. Those conditions are set out in Schedule 1, paragraph 4(2). This would cover, for example, an internal company message board that is contained within a public-facing service, but protected so that it is only accessible to the company's employees.

Clause 3: Meaning of "regulated service" and Schedule 1: Exempt services

33. This clause defines the term "regulated service". Subsections (3) and (4) set out that a "regulated service" is a user-to-user service or search service (both of which are defined in clause 2) which has links with the United Kingdom and is not exempt.

34. Subsections (5) and (6) clarify the circumstances under which the regulated service has links with the United Kingdom. A service will only be in scope if it has a significant number of users in the UK, if the UK is a target market, or if the service can be 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. As the regulatory framework established by the Bill is focused on protecting UK users, these subsections ensure that services which do not have UK links do not fall into scope of regulation.

35. Subsection (7) provides that services meeting the descriptions set out in Schedule 1 will be out of scope of regulation. This means that the following services will be exempt from regulatory duties: Email-only services, SMS and/or MMS-only services, services offering only one-to-one live aural communications, internal business services, limited functionality services and services provided by public bodies.

36. Subsection (8) allows the Secretary of State to make regulations which amend Schedule 1 in order to exempt additional user-to-user services or search services. This will provide for the Secretary of State to exempt new categories of services if the Secretary of State considers that the risk of harm to UK users presented by those services are low. Such categories could be based, for example, on the presence of only specific limited functionalities on a service. This power will allow the online safety framework to keep pace with technological and behavioural changes and to ensure that an excessive burden is not placed on UK businesses.

37. The power under subsection (9) enables some exemptions listed in Schedule 1 to be repealed, namely the exemptions for services offering one-to-one live aural communications, limited functionality services, and any exemptions created through the power set out in subsection (8). Exemptions can only be repealed subject to the condition in subsection (10), which is that the Secretary of State considers it is appropriate to do so because the category of exempt services poses a risk of harm to individuals in the United Kingdom. For the online safety framework to function effectively, it has to remain responsive to technological changes. Services which are currently low-risk, and which therefore merit a complete exemption from the framework today, may pose a higher risk of harm in the future. It is therefore important that these services can be brought into scope of the regulatory framework should the need arise.

38. Regulations can also be made to amend related provisions in Schedule 1 (see subsection (11)) or the definitions in clause 39 (“regulated content”, “user-generated content” and “search results"; see subsection (12)). The reason for this is that the development of new risks will not necessarily occur uniformly across exempt services and the functionalities they offer. It is possible that a risk could occur in relation to a specific functionality of an exempt service but not for another (such as in relation to comments rather than reviews). This power will mean that the entire exemption does not have to be repealed because of a localised risk in relation to a specific part of an exemption. This power provides the flexibility to respond to changing risks and technological developments without requiring the full repeal of an exemption.

39. Regulations under this clause are subject to the affirmative resolution procedure.

Schedule 1

40. Schedule 1 sets out which services will be exempt from regulatory duties. Subsection (7) of clause 3 (“Meaning of ‘regulated service’”) states that services of the descriptions set out in this Schedule are exempt.

41. Paragraphs 1, 2 and 3 explain that services will be exempt if the only type of user-generated content enabled by the service is, respectively, email, SMS and/or MMS

(as defined in clause 39(14)), or one-to-one live aural communications (as defined in clause 39(6)).

42. Paragraph 4 explains what is meant by “internal business service”, and states that such services are exempt from regulatory duties. The “internal business service” exemption encompasses services such as business intranets, productivity and collaboration tools, content management systems, customer relationship management systems and database management software.

43. To qualify as an internal business service, the service must meet the conditions set out in paragraph 4(2). These conditions are as follows. Firstly, the service must be an internal resource or tool for a business, or multiple businesses carried on by the same person. Secondly, the person carrying on the business (or businesses) must be the provider of the service, i.e. (for user-to-user services) the entity that has control over who can use the service and (for search services) the entity that has control over the operations of the search engine (see clause 116(2) and (5)). Thirdly, the service must only be available to a closed group of individuals. This may include (i) the person carrying on the business; (ii) the business’s officers (as defined in paragraph (4); (iii) the business’s employees or volunteers; and (iv) others who have expressly been authorised to use the service by an individual in (i), (ii) or (iii), such as a company contracted by the business.

44. Paragraph 4(3) states that an internal business search service is exempt from regulatory duties, even if only the search engine part of the search service meets the criteria in paragraph 4(2). A dissociable part of a user-to-user search service may qualify for this exemption (see subsection (6) of clause 2).

45. Paragraph 5 sets out that, under the limited functionality services exemption, a user-to-user service is exempt if the only functionalities enabling user-generated content on the service are the following:

    a. The posting of comment and reviews in relation to content that has been directly posted or uploaded by the service provider or website;

    b. The sharing of these comments and reviews on other internet services;

    c. Expressing views on such comments and reviews either through; (i): the “like or dislike” button, (ii): applying an emoji or symbol of any kind, (iii): engaging in yes/no voting and (iv): rating or scoring content.

    This exemption is expected primarily to exempt ‘below the line’ content on media articles and reviews of directly provided goods and services. Any services that meet the above requirements but have additional user-to-user functionalities will remain in regulatory scope.

46. Paragraph 6 provides that some user-to-user and search services provided by certain public bodies are exempt from regulatory duties. This exemption covers services provided by Parliament and foreign governments, as well as services provided by public authorities in the UK and bodies outside the UK where those services are provided in the exercise of functions of a public nature only.

Part 2: Providers of Regulated Services: Duties of Care

Chapter 1: Introduction

Clause 4: Overview of Part 2

47. The overview provides an outline of each of the Chapters contained within Part 2 of the Bill, which includes provisions relating to the duties of care applicable to providers of user-to-user services and search services, and for the issuing of codes of practice by OFCOM in relation to those duties.

Chapter 2: Providers of user-to-user services: Duties of care

Clause 5: Providers of user-to-user services: duties of care

48. This clause determines which of the duties set out in Part 2 apply to which regulated user-to-user services. The duties on search services are set out in the following chapter.

49. Subsection (2) lists the duties that all regulated user-to-user service providers must comply with, as follows:

    a. the illegal content risk assessment duty in clause 7;

    b. the illegal content duties in clause 9;

    c. the duty about rights to freedom of expression and privacy in clause 12;

    d. the applicable duties about reporting and redress set out in clause 15; and

    e. the record-keeping and review duties in clause 16.

50. Subsection (3) provides that certain additional duties will apply to providers of particular kinds of regulated user-to-user services as detailed in subsections (4) to (6).

51. Subsection (4) lists the additional duties that will be imposed upon all providers of a user-to-user service which is likely to be accessed by children (as is determined by the service provider in accordance with clause 26). These are:

    a. the duties to undertake children's risk assessments in clause 7;

    b. the duties to protect children's safety online in clause 10; and

    c. the relevant reporting and redress duties in clause 15 which apply in relation to content that is considered to be harmful to children.

52. Subsection (5) lists the additional duties to be imposed on providers of Category 1 services (the designation as a Category 1 service is determined by OFCOM's assessment under the provisions in clause 59). These are:

a. the duties to undertake adult risk assessments in clause 7;

b. the duties to protect adults' online safety in clause 11;

c. the duties to protect users' rights in clause 12;

d. the duties to protect content of democratic importance and journalistic content in clauses 13 and 14; and

e. the relevant reporting and redress duties set out in clause 15 relating to content that is harmful to adults and to the duties to protect content of democratic importance and journalistic content.

53. Where a user-to-user service includes a search engine, under subsection (6) the provider of the service must comply with the additional duties in relation to the search engine:

a. If the service is not likely to be accessed by children, then it must comply with the duties with regards to illegal content in clause 17(2).

b. If the service is likely to be accessed by children, then it must also comply with the duties with regards to illegal content and protecting children in clause 17(3).

Clause 6: Duties of care: supplementary

54. This clause makes it clear that the duties in this Chapter apply only to the design and operation of a user-to-user service as it affects users and others (such as individuals affected by content on services they do not themselves use) in the United Kingdom.

Clause 7: Risk assessment duties: user-to-user services

55. This clause sets out the risk assessment duties on regulated user-to-user services. These duties relate to assessing the risks arising from (i) illegal content, (ii) harm to children from content that is not illegal, and (iii) harm to adults from content that is not illegal. Not all regulated user-to-user service providers will have to risk assess against all such types of content.

56. Subsection (1) sets out the risk assessment duties in relation to illegal content that all regulated user-to-user service providers must comply with. These are:

a. to undertake an illegal content risk assessment;

b. to keep that risk assessment up to date; and

c. to update it before the service makes a significant change.

57. Subsection (3) relates to the children's risk assessment duties that regulated providers of services which are likely to be accessed by children (as assessed in accordance with clause 26) must adhere to. These are:

a. to undertake a children's risk assessment;

b. to keep that risk assessment up to date; and

c. to update it before the service makes a significant change.

58. Subsection (4) requires service providers to notify OFCOM about content they identify that is harmful to children that is not of a type specified in secondary legislation as primary priority or priority content that is harmful to children, as well as how often such content appears on the service.

59. Subsection (6) sets out the risk assessment duties for content that is legal but harmful to adults which providers of Category 1 services must comply with for those services. These are:

    a. to undertake an adults' risk assessment;

    b. to keep that risk assessment up to date; and

    c. to update it before the service makes a significant change.

60. Subsection (7) requires service providers to notify OFCOM about content they identify that is harmful to adults but which is not of a type specified in secondary legislation as priority content that is harmful to adults, as well as how often such content appears on the service.

61. Subsections (8) to (10) then define what the risk assessments for each of the three types of content should cover, and require that service providers must identify, assess and understand a number of factors (as appropriate) as set out in those subsections.

62. OFCOM will have a duty to issue guidance about risk assessments to assist providers of different types of services how to carry out their risk assessments: see clause 62. This will ensure providers have, for example, sufficient clarity about what a proportionate risk assessment looks like for their type of service and what would constitute a significant change that would require an updated risk assessment.

Clause 8: Timing of risk assessment under section 7

63. This clause sets out the time periods within which a regulated user-to user service provider must carry out the risk assessments referred to above. The time period will start to run from the day on which OFCOM publishes its report on its risk assessment under clause 61 and its guidance about risk assessments under clause 62, or if they are published on different days, whichever is the later of those days: see subsection (4). This is referred to as the "relevant day".

64. If the regulated user-to-user service was already operating immediately before the relevant day, they must carry out their risk assessments within three months unless they agree extra time with OFCOM: subsection (1). If the service provider begins operating after the relevant day then the risk assessment must be carried out before UK users are able to access the service: subsection (2). In the case of a user-to-user service which was not previously regulated but then becomes regulated, the relevant risk assessments must be carried out before users in the UK can access the service

or, if UK users can already access the service, as soon as possible after the service becomes regulated: sub-section (3).

Clause 9: Safety duties about illegal content

65. This clause sets out the duties on user-to-user services with regards to illegal content. As established by clause 5, all user-to-user services must comply with these duties.

66. Subsection (2) provides for a duty to take proportionate steps to reduce and manage the risk of harm to individuals identified in the illegal content risk assessment carried out under clause 7.

67. Subsection (3) requires service providers to use proportionate systems and processes designed to:

    a. Minimise the presence of priority illegal content on the service in the first place.

    b. Where priority illegal content is uploaded, to minimise the time for which it is present and its dissemination.

    c. Remove illegal content the service provider is made aware of, or becomes aware of, as soon as possible.

68. Subsections (4) and (5) impose obligations on providers to state in their terms of service how individuals are to be protected from illegal content, and then to ensure these terms are clear and accessible and applied consistently.

69. Subsection (6) specifies that whether steps, systems and processes in this case are proportionate will be determined by the levels of risk identified in the risk assessment and the service provider's size and capacity.

70. Subsection (8) links the duties about users' rights to freedom of expression and privacy in clause 12 to the illegal content safety duty in this clause.

Clause 10: Safety duties for services likely to be accessed by children

71. This clause sets out the duties on user-to-user services with regard to content that is harmful to children but is not illegal. As established in clause 5, user-to-user services that are likely to be accessed by children must comply with these duties.

72. Subsection (2) provides for a duty on services to take proportionate steps:

    a. to manage the risk of harm to children in different age groups from risks identified in the children's risk assessment as carried out under clause 7.

    b. to mitigate the impact of harm to children in different age groups from content that is harmful to children.

73. Subsection (3) requires service providers to use proportionate systems and processes, which are designed to:

a. Prevent children of any age from accessing primary priority content on their service, as defined in regulations to be made under clause 45.

b. Protect children in age groups which are judged to be at risk from other content that is harmful to children (being priority content as defined in regulations made under clause 45 and other content that satisfies the definition of content that is harmful to children) on their service.

74. Subsections (4) and (5) require providers to state in their terms of service how children are being prevented from encountering primary priority content on their service and how children are to be protected from encountering priority content that is harmful for children on their service, as set out in subsection (3). It also requires providers to set out how children are to be protected from encountering other content that would satisfy the definition of harmful to children. Providers must then ensure these terms are clear and accessible, and applied consistently.

75. Subsection (6) specifies that whether steps, systems and processes in this case are proportionate is determined by the levels of risk identified in the risk assessment and the service provider's size and capacity.

76. Subsection (7) makes clear that services are only required to fulfil the duty in this section in relation to non-designated content (i.e. neither primary priority content nor priority content, but content that would satisfy the definition of being harmful to children) if risks from non-designated content have been identified in the most recent children's risk assessment.

77. Subsection (8) explains that references in this clause to children judged to be in age groups at risk of harm from content that is harmful to children, are to be read as being those who have been assessed as such by the provider in their most recent children's risk assessment.

78. Subsection (9) clarifies that the duties in this section to protect children only extend to those parts of the service which it is possible for children to access, in line with the assessment on children's access set out in clause 26. For example, a service could have robust systems and processes, such as effective age verification measures, that ensure children are not normally able to access a part of the service.

79. Subsection (11) links the duties about users' rights to freedom of expression and privacy in clause 12 to the safety duties for services likely to be accessed by children.

Clause 11: Safety duties protecting adults: Category 1 services

80. This clause sets out the duties on Category 1 service providers with regards to content that is harmful to adults.

81. Subsection (2) provides for obligations to state in a provider's terms of service how content that is harmful to adults (as defined in clause 46) will be treated by the service provider on the Category 1 service in question. Subsection (3) requires that these terms of service must be both clear and accessible, and applied consistently.

82. Subsection (5) links the duties about users' rights to freedom of expression and privacy in clause 12 to the safety duty for content that is harmful to adults.

Clause 12: Duties about rights to freedom of expression and privacy

83. This clause sets out the duties about protecting users' rights in relation to user-to-user services.

84. Subsection (2) states that when designing and implementing their safety policies and procedures, all providers of regulated user-to-user services must have regard to the importance of protecting users' rights to freedom of expression and protecting users from unwarranted infringements of privacy.

85. Subsection (3) states that Category 1 service providers, additionally, have a duty to carry out an assessment of the impact that their safety policies and procedures will have on users' rights to freedom of expression and privacy. This applies to safety policies and procedures that they are considering and those that they have adopted on the Category 1 service.

86. Subsection (4) requires such service providers to publish these impact assessments and to keep them up to date.

87. Subsection (5) puts a duty on Category 1 service providers to state (either in their terms of service or in a publicly available statement) what steps they have taken with regard to the Category 1 service in question in response to the impact assessment set out in subsection (3).

88. References to users' rights to freedom of expression within the law include common law rights.

89. Subsection (6) confirms that the safety policies and procedures are those which are designed to ensure compliance with any of the safety duties and the reporting and redress duties in clause 15.

Clause 13: Duties to protect content of democratic importance: Category 1 services

90. This clause sets out the duties on providers of Category 1 services with regard to protecting content of democratic importance on those services.

91. Subsection (2) requires providers of Category 1 services to put in place systems and processes which ensure that the importance of the free expression of content of democratic importance is taken into account when making decisions on how to treat such content (especially decisions about taking it down or restricting users' access to it), and on how to treat users who generate or share it on their services.

92. Subsection (3) requires providers of Category 1 services to ensure that those systems and processes apply in the same way to a diversity of political opinion.

93. Subsection (4) requires providers of Category 1 services to specify in their terms of service how their policies and processes (particularly in relation to moderation decisions) are designed to take account of the importance of the free expression of content of democratic importance.

94. Subsection (5) states that those terms of service must be clear and accessible, and applied consistently.

95. Subsection (6) defines “content of democratic importance” as news publisher content or regulated content which is, or appears to be, specifically intended to contribute to democratic political debate in the UK or in any part or area of the UK. Examples of such content would be content promoting or opposing government policy and content promoting or opposing a political party.

96. Subsection (7) clarifies what is meant by ‘taking action’ against a user, while subsection (8) signposts the definitions of the terms “news publisher content” and “regulated content” in clause 39.

Clause 14: Duties to protect journalistic content: Category 1 services

97. This clause sets out the duties on providers of Category 1 services with regard to protecting journalistic content on those services.

98. Subsection (2) requires providers of Category 1 services to put in place systems and processes which ensure that the importance of the free expression of journalistic content is taken into account when making decisions on how to treat such content, and on how to treat users who generate or share it on their services

99. Subsection (3) requires a provider of Category 1 services to create a dedicated complaints procedure for users who generate, upload or share what they consider to be journalistic content on the service and creators of journalistic content, in relation to decisions by that provider to take down or restrict access to such content.

100. Subsection (4) requires a provider of Category 1 services to create a dedicated complaints procedure for users in relation to a decision by that provider to take action against a user because of content shared, uploaded or generated by the user which the user considers to be journalistic content.

101. Subsection (5) requires providers of Category 1 services to act swiftly to reinstate journalistic content and to reverse actions taken against users who have generated or shared journalistic content, where complaints under subsections (3) and (4) are upheld.

102. Subsection (6) imposes a duty on providers of Category 1 services to specify in their terms of service how they will identify journalistic content, how they will take into account the importance of the free expression of journalistic content when taking moderation decisions, and their policies and processes for handling complaints concerning journalistic content.

103. Subsection (7) provides that those terms of service must be clear and accessible, and applied consistently.

104. Subsection (8) defines “journalistic content” as content that is generated for the purposes of journalism, and which is ‘UK-linked’. Journalistic content encompasses regulated content and news publisher content. Subsection (9) defines the term “UK-linked”.

105. Subsection (10) clarifies what is meant by 'taking action' against a user and subsection (11) defines what is meant by the "creator" of journalistic content, while (12) signposts the definitions of the terms "news publisher content", "regulated content" and "recognised news publisher" in clause 39.

Clause 15: Reporting and redress duties

106. This clause sets out the user reporting and redress mechanisms, which apply to particular regulated user-to-user services as set out in clause 5.

107. Subsection (2) places a duty on services to have systems and processes in place that allow users or affected persons (as defined in subsection (7)) to report content that the user or affected person considers to be (a) illegal, (b) harmful to children (where that content can be accessed by a child), and (c) harmful to adults. All regulated providers must have systems in place for users or affected persons to report (a) illegal content, but beyond that, a service provider must only comply with the reporting duties that apply in relation to the content that is regulated on their service. For example, only providers of Category 1 services will have a duty to have a reporting mechanism for content that is harmful to adults on the Category 1 service in question, and only those services that are likely to be accessed by children will have reporting and redress duties in respect of content that is harmful to children. This is set out in clause 5.

108. Subsection (3) places a duty on the service to have a complaints procedure that is easy to access, easy to use and transparent, and that provides for the service provider to take appropriate action in response to the complaints set out in subsection (4). Where applicable, the complaints procedure must also be easy to access and use including for children who may wish to complain.

109. Subsection (4) outlines the kinds of complaints that subsection (3) applies to. This includes complaints about regulated content, complaints about a provider not complying with their safety duties or their duties in relation to freedom of expression and privacy, democratic content and journalistic content. This also includes complaints about action a provider has taken in relation to regulated content such as taking down or restricting access to that content and suspending or banning a user from using the service as a result of that content.

110. Subsection (5) places a duty on services to make their complaints policies and procedures publicly available and easy to access. This is to ensure that users and affected persons can easily find the complaints policies and procedures and that the process is transparent.

111. Subsection (6) provides that clause 26(3), which sets out when a provider is entitled to conclude that it is not possible for children to access a service, or part of a service, also applies for the purposes of the provisions in this clause which refer to the parts of a service which it is possible for children to access.

112. Subsection (7) defines an 'affected person' as someone other than a user of the service who is in the United Kingdom and is:

a. The subject of the content.

b. A member of a class or group of people with a certain characteristic targeted by the content.

c. A parent or other adult with responsibility for a child who is the user of the service or the subject of that content.

d. A person who is providing assistance in using the service to another adult who requires such assistance and who is a user of the service or the subject of the content.

113. Subsection (8) refers to the duties in respect of rights to freedom of expression and privacy in relation to the duties under this clause

Clause 16: Record-keeping and review duties

114. This clause sets out the record-keeping and review obligations that apply to regulated user-to-user services.

115. Subsection (2) puts a duty on providers to keep a written record of the risk assessments carried out under clause 7.

116. Subsection (3) requires providers to keep a written record of any steps they have taken to comply with the relevant duties listed in subsection (7) that are not provided for in the codes of practice which apply to that provider and service in question. This requirement does not apply where a service provider has followed steps set out in a code of practice.

117. Subsection (4) requires providers to review compliance with the relevant duties regularly and after making any significant change to the design and operation of their service.

118. Subsection (5) provides OFCOM with the ability to exempt certain providers from the need to keep written records. It is anticipated that this power could be used where there are small, low risk services. Under subsection (6) OFCOM must publish the details of any such exemptions.

Chapter 3: Providers of search services: duties of care

Clause 17: Providers of search services: duties of care

119. This clause is to be used to determine the duties which apply to all regulated search services (subsection (2)), and additional duties which are to apply where a regulated search service is likely to be accessed by children (subsection (3)).

120. All regulated search service providers must comply with the duties in relation to the illegal content risk assessment duty, each of the safety duties about illegal content, the duty to protect rights to freedom of expression and privacy, the user reporting and redress duties as they relate to illegal content and the Chapter 3 safety duties, and the record-keeping and review duties.

121. Where a search service is likely to be accessed by children (as should be determined by a service provider according to the assessment in clause 26), these services must comply with the children's risk assessment duty, each of children's safety duties, and the duties about reporting and redress that apply in relation to content that is harmful to children.

Clause 18: Duties of care: supplementary

122. Subsection (1) sets out that the duties described in this chapter are only applicable to the design and operation of search services so far as these may affect users and others who are in the United Kingdom.

123. To ensure the protection of journalistic freedoms, subsection (2) clarifies that the duties on search services are not applicable to content from recognised news publishers.

124. Subsection (3) provides that when a search engine forms part of a user-to-user service, the provisions in subsections (1) and (2) should be taken as applying to the search engine.

Clause 19: Risk assessment duties

125. This clause sets out the duties on regulated search services to assess risks arising from illegal content and content which is legal but harmful to children.

126. Subsection (1) places a duty on search services to undertake an illegal content risk assessment. Search services must undertake this within the time periods set out in clause 20. They must keep their risk assessment up-to-date and carry out a further risk assessment before making any significant changes to their service.

127. Subsection (2) refers to the children's risk assessment that services likely to be accessed by children must undertake. Search services must undertake this in accordance with the time periods set out in clause 20. They must keep their risk assessment up-to-date and carry out a further risk assessment before making any significant changes to their service.

128. Subsection (3) provides further detail on what would form part of an illegal content risk assessment. Service providers are required to identify, assess and understand the risk factors listed in this subsection (as appropriate), having regard to the risk profiles that relate to a service of its kind (risk profiles are those contained in OFCOM's guidance about risk assessments (clause 62)). The risk factors include the level of risk of users encountering terrorism content, child sexual exploitation and abuse (CSEA) content, priority illegal content, and other illegal content which can be accessed either on or via the search results of a search service. Service providers should take into account risks presented by algorithms and the way in which the service indexes, organises and presents search results.

129. Subsection (4) sets out the requirements of a children's risk assessment. Service providers are required to identify, assess and understand the risk factors listed in this subsection (as appropriate), having regard to the risk profiles that relate to a service of its kind (risk profiles are those contained in OFCOM's guidance about

risk assessments (clause 62)). The risk factors include the level of risk of children coming across primary priority, priority or non designated content in or via search results on the search service. Each kind of primary priority, priority and non designated content must be separately assessed. Further, the service provider must also give separate consideration to children in different age groups and take into account risks presented by algorithms used by the service and how the service indexes, organises and presents search results.

Clause 20: Timing of risk assessment under section 19

130. This clause sets out the time periods within which a regulated search service provider must carry out the risk assessments referred to above. The time period will start to run from the day on which OFCOM publishes its report on its risk assessment under clause 61 and its guidance about risk assessments under clause 62, if these are published on different days whichever is the later of those days: see subsection (4). This is referred to as the "relevant day".

131. If the regulated search service was already operating immediately before the relevant day, they must carry out their risk assessments within three months unless they agree extra time with OFCOM: subsection (1). If the service provider begins operating after the relevant day then the risk assessment must be carried out either before UK users are able to access the service: subsection (2). In the case of a user-to-user service which was not previously regulated but then becomes regulated, the relevant risk assessments must be carried out before users in the UK can access the service or, if UK users can already access the service, as soon as possible after the service becomes regulated: sub-section (3).

Clause 21: Safety duties about illegal content

132. This clause imposes duties on regulated search services with regards to illegal content.

133. Subsection (2) requires service providers to take proportionate steps to mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service.

134. Subsection (3) requires service providers to ensure they have proportionate systems and processes to minimise the risk of users encountering either priority illegal content or other illegal content that the provider knows about on their services because they have been alerted to it or they become aware of it in some other way.

135. Subsection (4) requires service providers to provide a publicly available statement explaining their policies and procedures for protecting users from illegal content. Subsection (5) requires those policies and procedures to be applied consistently and transparently.

136. Subsection (6) specifies that whether steps, systems and processes are proportionate is determined by the levels of risk identified in the risk assessment and the service provider's size and capacity. In practice, this means that the expectations will be different for a large, high risk service compared to a small, low risk service.

137. Subsection (8) links the duties about users' rights to freedom of expression and privacy in clause 23(2) to the illegal content safety duty in this clause.

Clause 22: Safety duties for services likely to be accessed by children

138. This clause imposes duties on regulated search services with regards to content that is harmful to children. As established in clause 17, regulated search services that are likely to be accessed by children must comply with these duties.

139. Subsection (2) requires service providers to:

a. take proportionate steps to manage the risk of harm to children in different age groups from risks identified in the children's risk assessment as carried out under clause 19; and

b. mitigate the impact of harm to children in different age groups from content that is harmful to children which they may encounter in or via search results.

140. Subsection (3) requires service providers to use proportionate systems and processes to minimise the risk of children of any age from encountering (in or via search results) primary priority content that is harmful to children. In the case of other content that is harmful to children, to minimise the risk of children encountering such content in or via search results where their age puts them at risk of harm, for example, protecting younger children encountering violent content which is not appropriate for their age.

141. Subsection (4) requires service providers to specify clearly in a publicly available statement details of their policies and procedures designed for protecting children from encountering primary priority content on their service and priority content that is harmful for children on their service. It also requires providers to set out how children are protected from encountering other content that would satisfy the definition of being harmful to children (see clause 45). Providers must then apply these policies and procedures consistently (subsection (5)).

142. Subsection (6) specifies that whether steps, systems and processes are proportionate is determined by the levels of risk identified in the children's risk assessment and the service provider's size and capacity.

143. Subsection (7) clarifies that services are only required to fulfil the duty in this section in relation to non-designated content (i.e. neither primary priority content nor priority content) if risks from the kinds of non-designated content that have been identified in the most recent children's risk assessment.

144. Subsection (8) clarifies that that the reference to 'age groups judged to be at risk of harm' are to those assessed as being so in the service provider's most recent children's risk assessment.

145. Subsection (9) clarifies that the above duties only apply to parts of the service accessible to children, in line with the assessment on children's access set out in clause 26.

146. Subsection (10) is self-explanatory.

147. Subsection (11) links the duties about users' rights to freedom of expression and privacy in clause 23(2) to the safety duties for services likely to be accessed by children in this section.

Clause 23: Duty about rights to freedom of expression and privacy

148. This clause sets out the duties on regulated search services to have regard to the importance of protecting users' rights to freedom of expression and protecting users from unwarranted infringement of privacy when designing and implementing their safety policies and procedures. References to freedom of expression within the law include common law rights.

Clause 24: Reporting and redress duties

149. This clause sets out the user reporting and redress mechanisms which apply to regulated search service providers.

150. Subsection (2) places a duty on service providers to have systems and processes in place that allow users or affected persons (as defined in subsection (6)) to report content encountered in or via search results that the user or affected person considers to be (a) illegal and (b) harmful to children (where that content can be accessed by a child).

151. Subsection (3) places a duty on the service provider to have a complaints procedure that is easy to access, easy to use and transparent, and that provides for the service provider to take appropriate action in response to the complaints set out in subsection (4). Where applicable, the complaints procedure must also be easy to access and use including for children who may wish to complain.

152. Subsection (4) outlines the kinds of complaints that subsection (3) applies to. This includes complaints about content that is considered to be illegal or harmful to children, which is encountered in or via search results, as well as complaints about a provider not complying with their safety duties or their duties in relation to freedom of expression and privacy. This also includes complaints by an interested party about action a service provider has taken (in complying with their safety duties) which results in content relating to an interested party no longer appearing in search results or being given a lower priority in the search results.

153. Subsection (5) places a duty on service providers to make their complaints policies and procedures publicly available and easy to access. This is to ensure that users, affected persons, and interested persons can easily find the complaints policies and procedures and that the process is transparent.

154. Subsection (6) defines an 'affected person' as someone who is in the United Kingdom other than a user of the service. An affected person is either:

a. The subject of the content.

b. A member of a class or group of people with a certain characteristic targeted by the content.

c. A parent or other adult with responsibility for a child who is a user of the service or the subject of that content.

d. A person who is providing assistance in using the service to another adult who requires such assistance and who is a user of the service or the subject of the content.

155. Subsection (7) links the duties about users' rights to freedom of expression and privacy in clause 23(2) to the duties in this clause.

Clause 25: Record-keeping and review duties

156. This clause sets out the record-keeping and review obligations that apply to the risk assessment duties, safety duties and the duties on reporting and redress above.

157. Subsection (2) requires service providers to keep a written record of the risk assessments carried out under clause 19.

158. Subsection (3) requires service providers to keep a written record of the steps they have taken to comply with the safety duties and reporting and redress duties that are not provided for in the codes of practice. This requirement does not apply where a service provider has followed steps set out in a code of practice.

159. Subsection (4) sets out a duty on service providers to review their compliance with the safety duties and duties on reporting and redress regularly and after making any significant changes to their service.

160. Subsection (5) provides OFCOM with the ability to exempt certain providers from the need to keep written records. It is envisaged that this could be used where there are small, low risk services. Subsection (6) requires OFCOM to publish the details of any such exemption.

Chapter 4: Assessment about access by children

Clause 26: Assessment about access by children

161. This clause establishes a requirement for providers of regulated services to conduct an assessment of whether children are likely to access their service. This is a key requirement of the safety duties to be imposed on all providers of regulated services in relation to children, as set out in clauses 10 and 22 (safety duties for services likely to be accessed by children).

162. Under subsection (1), the assessment must determine first, whether it is possible for children to access the service (or any part of it) and second, if so, whether (i) there are, in fact, a significant number of children who are users of the service or (ii) the service is of a kind likely to attract a significant number of users who are children. The second part of this assessment is known in the Bill as 'the child

user condition': see subsection (4). Subsection (9) provides more information about how the 'child user condition' is to be met.

163. Where a provider has more than one service, then an individual assessment as to whether it is likely to be accessed by children must be carried out for each service separately: subsection (2). For example, if a technology platform provides services which can be publicly accessible (e.g. public profiles) but also private (e.g. private messaging), two separate assessments will need to be conducted on the likelihood of children accessing each of these services.

164. Subsection (3) provides that a provider is only able to conclude that it is not possible for a child to access a service (or part of it), if there are robust systems and processes, such as effective age verification measures, in place that ensure that children are not normally able to access the service. Age verification refers to the age assurance measures that provide the highest level of confidence about a user's age. For example, where a regulated service hosts both user-generated content (which would be regulated content) and non-user generated content (which would not be regulated content), and its child users are only able to access the latter (e.g. a simple online game with age-gated messaging functionalities), then the provider would be able to conclude that its service is not likely to be accessed by children.

165. Subsection (5) provides that a service is to be 'treated as likely to be accessed by children' where the provider's assessment concludes that first, it is possible for children to access the service (or any part of it) and second, that either a significant number of children are using the service (or that particular part of it) or the service is likely to attract a significant number of users who are children (for example, if the design, functionality and content of the service is appealing to children).

166. Subsection (6) specifies that providers of services which are not 'likely to be accessed by children' must keep the assessment of children's access under review and complete a further assessment in three circumstances:

a. before making significant changes to the way their service functions (for example, if a new feature is introduced which may appeal to children);

b. where they are made aware of any issues with the effectiveness of their systems and processes for ensuring that children are not normally able to access the service;

c. where there is evidence of a significant increase in the number of children using the service.

167. Subsection (7) requires providers to keep written records of every assessment prepared in accordance with this clause, and subsection (8) provides that if a provider fails to carry out such an assessment, then that service will be treated as 'likely to be accessed by children' until such time as the provider carries out an assessment. Accordingly, the safety duties imposed on providers in relation to children will apply.

168. Subsection (9) provides more information about how the 'child user condition' is to be met. It establishes that for the purposes of the 'child user condition' a 'significant' number should be considered as such where it is significant in proportion to the total number of United Kingdom users of a service or (as the case may be) a part of a service. It also sets out that the 'child user condition' should be based on evidence about who actually uses a service, rather than who the intended users of the service are.

169. Subsection (10) is self-explanatory.

Clause 27: Timing of assessment under section 26

170. Subsection (1) requires existing regulated service providers to carry out their first assessment of whether children are likely to access their service within three months from the date OFCOM's guidance on making this assessment (see clause 28) is first published, unless agreed otherwise with OFCOM.

171. Subsection (2) requires providers of new user-to-user services or search services which start operating on or after the date referred to above, to carry out an assessment of whether children are likely to access the service before UK users are able to access the service. For user-to-user services or search services which become regulated services, an assessment must be carried out before users are able to access the service or, where UK users were already able to access the service, as soon as reasonably practicable after the service becomes a regulated service: see subsection (3).

172. Subsections (4) and (5) are self-explanatory

Clause 28: OFCOM's guidance about assessments under section 26

173. This clause will require OFCOM to produce and publish guidance for providers of services on how to make an assessment as to whether children are likely to access their services.

Chapter 5: Codes of practice

Clause 29: Codes of practice about duties

174. OFCOM is required to produce specific codes of practice in relation to the illegal content duties (set out in clauses 9 and 21) covering terrorist content (subsection (1)) and child sexual exploitation and abuse content (subsection (2)).

175. Subsection (3) requires OFCOM to prepare one or more codes of practice in relation to the relevant safety duties beyond those set out in subsections (1) and (2). How these codes should be structured and organised will be a matter for OFCOM to decide as appropriate. The codes of practice will set out the recommended steps that service providers can take to comply with the following relevant duties (see subsection (9)):

a. the safety duties for user-to-user services and search services;

b. the duties about democratic importance;

c. the duties about journalistic content; and

d. the duties about user reporting and redress.

176. To ensure the codes of practice stay up to date, subsection (4) allows OFCOM to prepare amendments and replacements to the codes of practice or to withdraw a code of practice.

177. When preparing codes of practice or amendments to them, subsection (5) sets out the parties whom OFCOM must consult. OFCOM must also consult those with expertise in national security or the enforcement of criminal law which is relevant to online safety matters dealing with illegal content (subsections (6) and (7)).

178. Subsection (8) sets out that the consultation requirements in subsections (5) and (6) are subject to exceptions where minor amendments are made to the codes of practice (as set out in clause 35).

Clause 30: Online safety objectives

179. Subsection (1) requires OFCOM to ensure that its codes of practice are compatible with the online safety objectives.

180. Subsection (2) sets out the objectives for user-to-user services and subsection (3) does the same for search services. For both types of services, the objectives set out that services are required to put in place effective and proportionate systems and processes for regulatory compliance and risk management. The objectives also set out that the functions and features of regulated services must be designed and operated to protect UK users from harm.

181. Subsection (4) makes provision for user-to-user services which include search services, providing that the objectives for search services apply to the search aspect of the user-to-user service.

182. Subsection (5) gives the Secretary of State a power to amend subsection (2) or (3) so as to vary the online safety objectives for regulated user-to-user services or regulated search services, by regulations. Should such amendments be made, subsection (6) obliges OFCOM, as soon as reasonably practicable, to consider whether a review of the codes of practice is required, and if any subsequent changes to the codes are needed following a review. Regulations made under this power are subject to the affirmative regulation procedure.

183. Clause 36(7) and (8) make further provisions about the role of the online safety objectives in relation to a service provider's compliance with the relevant duties. Providers who wish to comply with the duties in a way other than the steps set out in the codes of practice must have regard to the online safety objectives. On the issue of whether alternative steps taken by a provider are compliant, OFCOM is under a duty to consider the extent to which the alternative steps taken by the provider achieve the online safety objectives (so far as they are relevant to the service and the duty in question).

Clause 31: Further provision about codes of practice

184. Subsection (1)(a) requires OFCOM to consider how appropriate the steps within codes of practice are for the different kinds and sizes of regulated services and to different kinds, sizes and capacities of providers. Paragraph (b) then sets out various principles that OFCOM must follow when preparing a code of practice.

185. Subsection (2) allows codes of practice to make provisions that are different for user-to-user and search service providers, and to make different provisions for different types of user-to-user providers. It also allows OFCOM to differentiate between regulated services and between providers, as appropriate.

186. Subsection (3) provides that codes of practice can apply to providers based outside of the United Kingdom.

187. Subsection (4) provides that steps set out in a code of practice may only relate to the design or operation of regulated services as they affect users and others in the United Kingdom. This means that OFCOM could not set out steps which relate to the design or operation of services which do not affect UK users.

188. Steps within the codes of practice must be designed with the importance of users' rights to free expression and privacy in mind, and incorporate safeguards for these rights, where appropriate: see subsections (5) and (6).

Clause 32: Approval of codes of practice

189. The next three clauses set out the procedural requirements for approval and publication of the codes of practice.

190. Subsections (1) and (2) set out that OFCOM must submit a code of practice to the Secretary of State, and provided the Secretary of State does not intend to issue a direction to OFCOM (see clause 33), the Secretary of State must lay the code before Parliament.

191. Subsection (3) provides that, once the code of practice has been laid before Parliament, Parliament has 40 days to resolve not to approve it. If Parliament resolves not to approve the code of practice, OFCOM must not issue the code and must prepare another version of it.

192. Subsection (4) provides that if Parliament does not make such a resolution, OFCOM must issue the code of practice and it will come into force after 21 days (beginning on the day on which it is issued).

193. Subsection (5) defines "the 40-day period" in which Parliament may resolve not to approve the code or practice. This period is defined as starting when the code has been placed before both Houses of Parliament. Subsection (6) further specifies that in calculating this period, days when Parliament is dissolved or prorogued or both Houses are adjourned for more than 4 days should not be taken into account.

194. Subsection (7) provides that this clause applies to amendments to a code of practice prepared under clause 29. Subsection (8) provides that this clause is subject

to clause 35, which sets out the process for making minor amendments to codes of practice.

Clause 33: Secretary of State's power of direction

195. Subsection (1) confers a power on the Secretary of State to direct OFCOM to modify a code of practice submitted to the Secretary of State under clause 32(1). This subsection further specifies that the Secretary of State may use this power if they believe that modifications are required to reflect government policy; or, in respect of the child sexual exploitation and abuse and terrorism codes only, for reasons of national security or public safety.

196. Subsection (2)(a) qualifies this power of the Secretary of State by providing that a direction made under this clause cannot require OFCOM to include a particular step recommended to be taken by providers of regulated services in a code of practice. Subsection (2)(b) further qualifies this power by providing that the Secretary of State must give reasons for requiring modifications, except where setting out those reasons would be against the interests of national security or the UK's relations with the government of another country.

197. Subsection (3) provides that OFCOM must as soon as reasonably practicable comply with a direction made under this clause and sets out the steps that OFCOM must take when sending the modified code back to the Secretary of State. OFCOM would be required to submit a document to the Secretary of State containing details of the direction and changes that have been made to the code of practice as a result of the direction. OFCOM must also inform the Secretary of State of any modifications that have been made that are not in response to a direction.

198. Subsection (4) provides that the Secretary of State may make further directions. Any further directions must also be issued for one of the reasons set out in subsection (1) and the requirements in subsections (2) and (3) will apply.

199. Under subsection (5), once the Secretary of State is content that no further modifications are necessary, they must as soon as reasonably practicable lay the revised code of practice before Parliament along with any document submitted by OFCOM that details what changes have been made to the code of practice, as mentioned in subsection (3)(c).

200. Subsection (6) provides that the negative resolution procedure set out in subsections (3) to (6) of clause 32 also applies in relation to modified codes of practice that have been laid before Parliament in accordance with subsection (5). Subsection (7) provides that the process set out in this clause also applies to amendments to a code of practice submitted to the Secretary of State under clause 32.

Clause 34: Publication and review of codes of practice

201. This clause sets out what OFCOM must do once a code is ready for publication. Subsection (1) provides that OFCOM must publish a code of practice issued under clause 32 within 3 days of it being issued.

202. Subsection (2) provides that where amendments of a code of practice have been issued, OFCOM must publish the amended code within 3 days beginning with the day on which the amendments are issued.

203. Subsection (3) applies when a code of practice has been withdrawn, and requires OFCOM to publish a notice setting out that the code has been withdrawn.

204. Subsection (4) provides that publication of a code of practice under this clause must be in any manner that OFCOM considers appropriate.

205. Subsection (5) provides that OFCOM must keep each code of practice published under this clause under review, and subsection (6) provides that the Secretary of State may require a review by OFCOM of either the terrorism or the child sexual exploitation and abuse (CSEA) code of practice at any time under section 29(1) or (2), and if any amendments are required this will be subject to the process for amendments as provided in clause 29.

Clause 35: Minor amendments of codes of practice

206. This clause allows OFCOM to make minor amendments to the codes of practice (for example to reflect the changes of the name of a relevant organisation) without needing to comply with the requirements for consultation and parliamentary scrutiny. This flexibility should allow the codes to remain up-to-date.

207. Subsection (1) explains that this clause applies when OFCOM proposes amendments to a code of practice and OFCOM considers that the minor nature of the amendments means that consultation is unnecessary and the amendments should not be required to be laid before Parliament.

208. Subsection (2) provides that OFCOM must notify the Secretary of State of these proposed amendments. Subsections (3) provides that, if the Secretary of State agrees that it is appropriate, the amendments may be made and issued without complying with the requirements of clause 29(5) and (6) or clause 32. This means that OFCOM does not have to consult on the proposed changes and the amended codes do not need to be laid before Parliament.

209. Subsection (4) provides that if the Secretary of State agrees with OFCOM that the changes are minor and do not require consultation or to be laid before Parliament, OFCOM may prepare and issue the amendments of the code of practice.

210. Subsection (5) provides that amendments issued under this clause come into force at the end of 21 days, beginning with the day on which the amendments are issued.

211. Subsection (6) provides that amendments of a code of practice issued under this clause must be published within three days of issue.

Clause 36: Relationship between duties and codes of practice

212. This clause sets out how providers can comply with their relevant duties under this Bill.

213. Subsection (1) provides that a provider of a regulated user-to-user service will be treated as complying with their safety duties for protecting children and adults, reporting and redress duties, and duties related to journalistic content and democratic content if it takes the steps set out in the relevant codes of practice which are recommended for compliance with the duty in question.

214. Subsection (2) provides that, in relation to the safety duties for illegal content, a provider of a regulated user-to-user service will be treated as having complied with them if it has taken the recommended steps and OFCOM is also satisfied that terrorist content and CSEA content are not prevalent, and are not persistently present, on its services.

215. Subsection (3) provides that a provider of a regulated search service is to be treated as complying with its safety duties in relation to children and reporting and redress duties if the provider takes the relevant steps described in a code of practice which are recommended for the purposes of compliance with the duty in question.

216. Subsection (4) provides that a provider of a regulated search service is to be treated as compliant with the safety duties about illegal content if it takes the relevant steps described in the codes of practice that are recommended for the purposes of compliance with the duty in question. In addition, OFCOM must be satisfied that terrorism and CSEA content is not prevalent, and is not persistently present, in the search results of the search service.

217. Subsection (5) specifies when a provider of a regulated user-to-user service is to be treated as complying with the duty set out in clause 12(2) (which is to have regard to the importance of freedom of expression and privacy when implementing safety policies and procedures). A provider will be treated as complying with this duty if they take steps described in a code of practice that are recommended for compliance with their safety duties which incorporate safeguards for the protection of users' rights to freedom of expression or the protection of users from unwarranted infringements of privacy.

218. Subsection (6) specifies when a provider of a regulated search service is to be treated as complying with the duty set out in clause 23(2) (which is a duty to have regard to the importance of freedom of expression and privacy when deciding on and implementing safety policies and procedure). A provider will be treated as complying with this duty if they take steps described in a code of practice that are recommended for compliance with their safety duties which incorporate safeguards for the protection of the rights of users and interested persons to freedom of expression or the protection of users from unwarranted infringements of privacy.

219. Subsection (7) provides that non-compliance with a provision in a code of practice does not by itself make the provider liable to legal proceedings in a court or a tribunal.

220. Subsection (8) provides that a provider of a regulated service who seeks to comply with a relevant duty by acting otherwise than by taking a step described in a code of practice must have regard to the following:

a. The online safety objectives (in clause 30) where these are relevant to the service and duty in question; and

b. Where relevant, the importance of protecting the rights of users (and, for search services, interested persons) to freedom of expression and from unwarranted infringements of privacy.

221. Subsection (9) provides that, when assessing whether a provider of a regulated service is compliant with a relevant duty where they have acted otherwise than by taking a step described in a code of practice, OFCOM must consider whether the alternative steps taken by the provider:

a. Achieve the online safety objectives (in clause 30) so far as they are relevant to the service and duty in question: and

b. Where appropriate, incorporate appropriate safeguards protecting the rights of users to freedom of expression and from unwarranted infringements of privacy.

222. Subsection (10) provides that in subsections (3), (4) and (6), references to a provider of a regulated search service also include a provider of a regulated user-to-user service that includes a search engine.

223. Subsection (11) defines various terms used in this clause, which are self explanatory.

Clause 37: Effect of codes of practice

224. Subsection (1) provides that codes of practice can be used as evidence in legal proceedings.

225. Subsection (2) provides that a court or tribunal must take into account a provision of a code of practice, when determining a question that arises during legal proceedings if (i) the question relates to a time when the provision was in force and, (ii) the provision appears to the court of tribunal be relevant to the question.

226. Subsection (3) requires OFCOM to take into account a provision of a code of practice, when determining a question which arises in connection with their exercise of any relevant function (defined in subsection (4)) if (i) the question relates to a time when the provision was in force and (ii) the provision appears to OFCOM to be relevant to the question.

227. Subsection (4) is self-explanatory.

Clause 38: Duties and the first codes of practice

228. Subsection (1) provides that the duties identified in subsection (2) apply to providers of regulated services from the day on which the first code of practice relating to each duty comes into force.

229. Subsection (3) defines the criteria for when a code of practice is the first relating to a duty. These are:

a. It sets out the recommended steps for complying with that duty; and

b. It is the first code of practice that defines the steps for those purposes.

230. Subsections (4) and (5) make specific provision for the relevant duties in relation to illegal content (as they apply to terrorism and CSEA. These duties apply when the first codes on terrorism and CSEA come into force. Subsection (6) modifies subsection (1) of this clause accordingly.

231. Subsection (7) makes clear that for particular providers of regulated services the provisions of this clause only concern the duties which apply to them (as specified in clause 5 for providers of user-to-user services, and in clause 17 for providers of search services). So for example, the duty to protect content of democratic importance will apply only to providers of Category 1 services when the relevant code of practice comes into force.

Chapter 6: Interpretation of Part 2

Clause 39: Meaning of "regulated content", "user-generated content" and "news publishers content"

232. This clause defines "regulated content" and "user-generated content". It establishes that "regulated content" is a subset of "user-generated content", and describes the types of user-generated content which do not count as "regulated content".

233. Subsection (2) states that "regulated content" on user-to-user services is user-generated content, with the exception of the types of content listed in paragraphs (a) to (g).

234. The safety duties imposed on the provider of a regulated service will not cover the types of user-generated content which are exempt from the definition of "regulated content". For example, a social media service will be a regulated service, but the provider of the service will not have duties with regards to the types of user-generated content listed in paragraphs (a)-(g) of subsection (2). This differs from the exemptions established in clause 3 and Schedule 1, which exempt whole types of services from the scope of the regulatory framework.

235. Subsection (3) defines "user-generated content" as content that is generated by a user of the service, or uploaded to or shared on the service by a user of the service, and which may be encountered by another user (or users) by means of the service. For example, this would include anything posted on a forum or social media network; a direct message from one user to another; or a file stored in shared cloud storage.

236. "User-generated content" does not include content published by the service provider. For example, a blog posted by someone on their own site, a press release posted by a company on its own site, or a television programme published by a broadcaster on its own streaming app would not count as user-generated content.

237. Furthermore, “user-generated content” does not include content uploaded by a user which may not be encountered by any other users. For example, content shared only between a user and the service provider (such as through a customer service chat function) would not fall under the definition of user-generated content.

238. Subsection (4) provides additional detail for the purposes of subsection (3). Subsection (4)(a) establishes that content which is generated, uploaded or shared by means of software or an automated tool applied by the user counts as “user-generated content”. For example, if a user used a tool for content to be uploaded automatically at a later date, the content would still count as user-generated content. Equally, if a user uploaded content to Service A, and applied a tool which automatically also shared it to Service B, the content would count as user-generated content on both Service A and Service B.

239. Subsection (4)(b) establishes that for these purposes a bot counts as a user if it interacts with user-generated content, as long as it is not operated by or on behalf of the provider. For example, a bot unconnected with the provider of a service which posted content on that service would count as a user (and the content would therefore count as “user-generated content”). However, a bot operated by the service provider posting updates to the provider’s service, would not count as a user of that service, and therefore the content posted would not count as “user-generated content”.

240. Subsection (5) defines “comments and reviews on provider content” in respect of user-to-user services; this relates to the exemption under subsection (2)(d). This definition encompasses user comments and reviews in relation to all content that is directly uploaded by a service provider. In practice, this exemption will primarily benefit ‘below the line’ comments on articles on news publisher’s sites and user reviews on directly advertised products and services. This exemption will not apply to comments on or reviews of user-generated content such as goods and services advertised by third party sellers on online marketplaces.

241. Subsection (6) defines “one-to-one live aural communications”; this relates to the exemption in subsection (2)(e). It makes clear that only aural communications between two users which are not accompanied by written messages, videos or other visual images, and which are not recordings of such content, are exempt from the definition of “regulated content”. For example, a one-to-one live voice call over an internet service would not count as “regulated content”, but a one-to-one video call or a recording of a call shared on a regulated service would.

242. Subsection (7) defines “paid-for advertisements”; this relates to the exemption in subsection (2)(f). To count as a “paid-for advertisement”, firstly the service provider must receive “consideration” of any sort (such as money, a gift, or data) for the advertisement. That consideration may come directly from the advertising party, or may come indirectly, for example through an intermediary company. Secondly, the advertisement must be placed by systems or processes that are agreed between the contracting parties. Such systems and processes may be human (for example, an agreement to place an advert in a particularly prominent place on a service) or

automated (for example, through an algorithm which tailors adverts to specific types of users).

243. Subsections (8) to (10) define "news publisher content"; this relates to the exemption in subsection (2)(g). Under subsection (9), content on a service directly generated by a recognised news publisher (as defined in clause 40) does not count as user-generated content. Under subsection (10), content originally published by a recognised news publisher but uploaded to or shared on a service by another user of that service, either in its entirety or by way of a link to the entirety of the material, also does not count as user-generated content. For example, if a user shares the text of an article copied from a recognised news publisher's website, with no additions or amendments, that text will not count as user-generated content. If content generated by a recognised news publisher that has been amended by another user is uploaded to or shared on the service by another user it will count as user-generated content. For example, if a user shares only part of an article, the extract shared will count as user-generated content. Any commentary about the article shared at the same time as the article also counts as user-generated content. Equally, if an image of content generated by a recognised news publisher is uploaded to or shared on a service by another user that image will also count as user-generated content.

244. Subsection (12) confers a power on the Secretary of State to repeal by regulations the exemption for comments and reviews on provider content, if the Secretary of State considers that it is appropriate to do so because of the risk of harm to individuals presented by this type of user-generated content. Subsection (13) confers an equivalent power in relation to one-to-one live aural communications. In both cases, regulations would be subject to the affirmative procedure.

Clause 40: Meaning of "recognised news publisher"

245. This clause defines the term "recognised news publisher".

246. Subsection (1) states that the British Broadcasting Corporation, Sianel Pedwar Cymru, and any entity that holds a license under the Broadcasting Act 1990 or 1996 and which publishes news-related content under that license will qualify as a recognised news publisher. Subsection (1)(d) adds that any entity that meets the conditions listed in subsection (2) will also be considered a "recognised news publisher", providing it is not excluded under subsection (3).

247. Subsection (2) then sets out the conditions that other entities have to meet in order to be considered a "recognised news publisher" under subsection (1)(d).

248. Subsection (3) sets out the conditions in which an entity is excluded from the definition of "recognised news publisher", even where it otherwise meets the criteria set out in subsection (2). These are that the entity is a proscribed organisation under the Terrorism Act 2000 or is an entity which supports such an organisation.

249. Paragraph (a) of subsection (4) defines the conditions in which news-related material can be said to be "subject to editorial control". This relates to the conditions for a "recognised news publisher" in subsection (2). The term "control" is defined in

paragraph (b) by reference to section 202 of the Broadcasting Act 1990, which itself refers to the detailed provisions in paragraph 1(1) of Part 1 of Schedule 2 to that Act.

250. Subsection (5) defines the terms “news-related material”, “publisher” and “standards code”.

Clause 41: Meaning of “illegal content”

251. This clause defines illegal content using the concept of content which amounts to a relevant offence (subsections (2) and (3)). Content amounts to a relevant offence if the provider of the service has reasonable grounds to believe that the use of the words, images, speech or sounds in the content (either in itself or when taken together with other content present on the service) amounts to a relevant offence, or that the dissemination of the content constitutes a relevant offence.

252. Subsection (4) defines a “relevant offence” as a terrorism offence (see clause 42), a child sexual exploitation and abuse (CSEA) offence (see clause 43), an offence which the Secretary of State has specified in regulations under clauses 41 and 43, or another offence which has or is intended to have one or more individual victims. Only offences under the law of any part of the United Kingdom can be relevant offences (subsection (9). Examples of relevant offences that are not terrorism or CSEA offences include revenge pornography, the sale of illegal goods, and upskirting.

253. Subsection (5) clarifies that when the relevant offence is a terrorism offence or a CSEA offence, the content is described as terrorism content or CSEA content respectively. This subsection also clarifies that when the relevant offence is specified in regulations it is described as priority illegal content.

254. Subsection (6) excludes certain categories of offence from the definition of illegal content. These are offences involving infringements of intellectual property rights, unsafe or substandard goods and services provided by an unqualified provider.

255. To reflect the difficulty of determining where online content is generated, subsection (7) provides that, when determining whether content amounts to an offence, no account is to be taken of whether or not anything done in relation to that content takes place in the United Kingdom.

256. Subsection (8) clarifies that illegal content, terrorism content, CSEA content and priority illegal content does not have to be present on a regulated service to meet the relevant definitions for these types of content. This provision is necessary to allow service providers to take steps in relation to content which would not otherwise meet the definitions because it had not yet been uploaded to or shared on their services.

Clause 42: Offences relating to terrorism

257. This clause refers to Schedule 2 to the Bill, which defines the offences that constitute “terrorism content”.

258. They are based in existing domestic legislation, including from the Terrorism Act 2000 and 2006, and the Anti-terrorism, Crime and Security Act 2001. The Bill does not introduce any new offences.

259. The Secretary of State can amend Schedule 2 through regulations.

Schedule 2

260. Schedule 2 defines the offences that constitute “terrorism content”.

261. Paragraph 1 lists the relevant provisions that apply from the Terrorism Act 2000, and Paragraph 3 lists the relevant provisions from the Terrorism Act 2006

262. Paragraph 2 sets out the relevant section from the Anti-terrorism, Crime and Security Act 2001.

263. Paragraph 4 sets out, for the purpose of this Schedule, an inchoate offence as:

a. An offence of attempting to, or conspiring to, commit any of the offences set out above.

b. An offence under Part 2 of the Serious Crime Act 2007 in relation to any of the offences set out above. In Scotland, this would also include inciting a person to commit such offence.

c. An office of aiding, abetting, counselling or procuring the commission of an offence set out above. In Scotland, this includes being involved, art and part, in commissioning of such an offence.

Clause 43: Offences relating to child sexual exploitation and abuse

264. This clause refers to Schedule 3 to the Bill, which defines the child sexual exploitation and abuse (CSEA) offences that apply to this Bill.

265. They are based on existing legislation for CSEA offences which applies in England and Wales, Scotland and Northern Ireland. The Bill does not introduce any new offences.

266. The Secretary of State can amend Part 1 or 3 of Schedule 3 and Scottish Ministers can amend Part 2 of Schedule 3 through regulations.

Schedule 3

267. Schedule 3 defines the child sexual exploitation and abuse offences that apply to this Bill. Part 1 applies to England and Wales, Part 2 applies to Scotland, and Part 3 applies to Northern Ireland.

Clause 44: Regulations under section 41

268. This clause sets out the matters to be taken into account by the Secretary of State when making regulations specifying relevant offences for the purpose of defining illegal content.

269. Subsection (1) requires the Secretary of State to take account of the prevalence of the offence on regulated services, the risk of harm to individuals in the UK and how severe that harm is likely to be.

270. Subsections (2) to (6) make equivalent provision in relation to offences as is made in subsections (3), (6) and (7) of clause 41.

Clause 45: Meaning of “content that is harmful to children” etc

271. This clause defines “content that is harmful to children”.

272. Subsection (2) defines “content that is harmful to children”. It defines this as regulated content (see clause 39) which the Secretary of State has designated in regulations (see clause 47) as either primary priority or priority content which is harmful to children, or which meets the conditions of subsections (4) or (6) of this clause.

273. Subsection (3) states that content is in scope of regulation if the provider has reasonable grounds to believe that the nature of the content risks directly or indirectly having a significant adverse physical or psychological impact on a child of ordinary sensibilities. This could be by indirectly resulting in physical injuries or by directly or indirectly resulting in a significant negative effect on the mental state of an individual. This could include causing feelings such as serious anxiety and fear; longer-term conditions such as depression and stress; and medically recognised mental illnesses, both short-term and permanent.

274. Subsection (4) provides that, where harmful content would reasonably be assumed to particularly affect people with certain characteristics or belonging to a certain group, for example people with disabilities or people of a particular religion, the provider should assume that the child encountering that content possesses those characteristics or belongs to that group.

275. Subsection (5) provides that content may be harmful to children due to the way in which it is disseminated, even if the nature of the content is not itself harmful, for example, repeatedly sending apparently innocuous content to a user could be bullying or intimidating. In determining whether content is harmful to children, a provider should also take into account how many users could be encountering the content on the service and how easily, quickly and widely the content can be disseminated on the service.

276. Subsection (6) clarifies that for the purposes of (3) and (5), the provider should assess the impact on a child of ordinary sensibilities with reference to children across the age range. Content is to be regarded in scope of (3) and (5) if the provider has reasonable grounds to believe that there is a risk of harm to children of any particular age.

277. Subsection (7) provides that where the provider has knowledge about the child that content in scope of subsections (3) and (5) is directed at, or if the child is the subject of the content, subsections (3) to (5) should be read in reference to that particular child instead of a child of ordinary sensibilities, taking into account that child's characteristics or membership of a certain group of people, where known or inferred by the provider.

278. Subsection (8) sets out that content could 'indirectly' cause harm as described in subsection (3) where it causes an individual to do or say things to a targeted child that would have a significant adverse physical or psychological impact on that child, or where it causes a child to act in a way which has, or increases the likelihood, of a significant adverse physical or psychological impact on that child (for example, content which promotes risky or violent behaviour).

279. Subsection (9) sets out content that should not be regarded as within subsections (3) or (5), namely illegal content or content where the risk of physical or psychological harm comes from the content's potential financial impact, the safety or quality of goods featured in the content, or the way in which a service featured in the content may be performed.

280. Subsections (10) - (12) set out definitions for the purposes of this clause.

Clause 46: Meaning of "content that is harmful to adults" etc

281. This clause defines "content that is harmful to adults".

282. Subsection (2) defines "content that is harmful to adults" on Category 1 services. It defines this as regulated content on a service (see clause 39), which is either priority content, designated as such by the Secretary of State in regulations (see clause 47), or which meets the conditions of subsections (3) and (5).

283. The remainder of this clause contains equivalent provisions to those in subsections (3) to (5) and (7) to (12) of clause 45.

Clause 47: Regulations under sections 45 and 46

284. This clause makes provision in relation to the making of regulations under clauses 45 and 46 designating primary priority and priority content that is harmful to children, and priority content that is harmful to adults. It also sets out requirements for OFCOM to review and report on their efficacy.

Clause 48: Meaning of "Chapter 2 safety duty" and "Chapter 3 safety duty"

285. This clause signposts the sections relevant to the key terms used in Part 2 of the Bill.

Part 3: Other Duties of Service Providers

Chapter 1: Transparency Reports

Clause 49: Transparency reports by service providers

286. This clause requires providers of relevant services to publish annual transparency reports and sets out OFCOM's powers in relation to these reports. The information set out in transparency reports will help ensure that users are able to understand the steps providers are taking to keep them safe, and will furnish OFCOM with the information required to hold them to account where needed.

287. Subsection (1) requires providers of relevant services to produce annual transparency reports. This report must contain the information of a kind specified by OFCOM in a notice given to the provider, in the format specified by OFCOM, and must be submitted by a date specified by OFCOM and published in the manner and by the deadline given by OFCOM.

288. Subsection (2) requires providers of relevant services to ensure that the information in their transparency reports is complete and accurate.

289. Subsection (3) provides that only Category 1, Category 2A and Category 2B services will be classified as "relevant services", and thus only providers of these services will be required to produce annual transparency reports. The subsection also signposts to clause 59(6) for more information on the definitions of Category 1, Category 2A and Category 2B services.

290. Subsection (4) specifies the types of information that OFCOM will be able to require providers of relevant services to include in their transparency reports. This could include, for example, information about the incidence of harmful content on a provider's service and the processes enabling users to report such content. The subsection describes high-level types of information in order to allow OFCOM the flexibility to tailor the exact information it will require to the relevant service in question. Moreover, in order to ensure that the types of information that can be required remain relevant to a fast-changing online safety landscape, subsection (7) permits the Secretary of State, having consulted OFCOM, to amend the types of information listed in subsection (4) by regulations.

291. Subsection (5) sets out various factors that OFCOM must take into account when deciding which types of information to require under subsection (4). These include the service provider's capacity to produce information, the type of service and the functionalities the service offers, the number of UK users of the service and the proportion of UK users who are children. These factors are designed to help OFCOM to select the most appropriate and proportionate types of information to require from the service provider in question

292. Subsection (6) grants the Secretary of State the power to change (via regulations) the frequency with which providers of relevant services are required to produce transparency reports. The Secretary of State must consult OFCOM before making regulations under this subsection (subsection (8)).

293. Subsection (7) grants the Secretary of State the power to change (via regulations) the kinds of information that OFCOM can require a provider of a relevant service to include in its transparency report under subsection (4), and the factors that OFCOM must take into account under subsection (5) in deciding which kinds of information to require. The Secretary of State must consult OFCOM before making regulations under this subsection (subsection (8)).

294. Subsection (9) signposts to the meanings of the terms "content that is harmful to adults", "content that is harmful to children" and "illegal content".

Clause 50: Transparency reports: guidance

295. This clause places a requirement on OFCOM to prepare guidance on how it will exercise its powers relating to transparency reports (clause 49) and to consult on and publish this guidance.

296. Subsection (1) places a duty on OFCOM to prepare guidance detailing, for example, how it will decide what types of information (from the list in clause 49(4)) it will require providers of relevant services to include in their transparency reports, describing how information from provider's transparency reports will be used in drawing up OFCOM's transparency report, and anything else that OFCOM deems relevant to the production and publication of providers' transparency reports and its own transparency report.

297. Subsection (2) sets out a list of people whom OFCOM must consult before preparing guidance, if OFCOM considers it appropriate to consult that person.

298. Subsection (3) requires OFCOM to publish the first version of the guidance, as well as any later versions of the guidance.

299. Subsection (4) says that in exercising its functions under section 49 or 100, OFCOM must have regard to the guidance for the time being in force under this section.

300. Subsection (5) notes that the term "relevant service" means the same thing in this clause as it does in clause 49.

Chapter 2: Fees

Clause 51: Duty to notify OFCOM

301. This clause specifies that providers with qualifying worldwide revenue at or above a specified threshold will have an obligation to notify OFCOM and pay an annual fee, as described in clause 52. Where providers whose qualifying worldwide revenue is at or above the threshold do not notify or pay a fee, then enforcement action may be taken against them as provided for in clauses 88 and 89.

302. Subsection (1) specifies that a provider must notify OFCOM for the first charging year that the provider is required to pay a fee. This may be the initial charging year or a subsequent charging year. The provider must also notify OFCOM where they believe they are no longer liable to pay a fee.

303. Subsection (2) clarifies that a "fee paying year'' for a provider means a charging year where the provider is not exempt from paying a fee, and where their qualifying worldwide revenue for the relevant time period is at, or above, the threshold set by OFCOM for that year.

304. Subsection (3) specifies that at the point of notification, the provider must share with OFCOM:

a. details of the regulated service(s) they provide;

b. its qualifying worldwide revenue for the relevant time period; and

c. any other relevant information requested by OFCOM and specified in OFCOM's Statement of Charging Principles (i.e. the document issued annually by OFCOM which includes key information on how funding is allocated to OFCOM itself and what principles are followed in determining fees to be charged): see clause 55.

305. Subsection (4) clarifies that providers will need to notify OFCOM within timeframes detailed in OFCOM's Statement of Charging Principles.

306. Subsection (5) allows for OFCOM to exempt particular descriptions of providers from these notification requirements and the duty to pay a fee as described in clause 52. The exemption must be approved by the Secretary of State.

307. Subsection (6) allows for OFCOM to revoke any exemption specified in subsection (5), as long as the revocation has been approved by the Secretary of State.

308. Subsection (7) requires that OFCOM must publish details of any exemption approved under subsection (5).

309. Subsection (8) gives the Secretary of State the power to make regulations to define "qualifying worldwide review" and "qualifying period".

310. Subsection (9) requires that the Secretary of State consult OFCOM before making the regulations under subsection (8).

311. Subsection (10) clarifies that for the purposes of notification and payment of an annual fee, a "provider of a regulated service" can include providers who have been providing a service for either the entire year, or part of the year.

312. Subsection (11) defines "charging year'' and "initial charging year''.

Clause 52: Duty to pay fees

313. This clause sets out the factors taken into account by OFCOM when determining which regulated services are required to pay the fee, and the level of the fee to be paid.

314. Subsection (1) enables OFCOM to charge a fee to providers of a regulated service so long as the provider is not exempt and the provider's qualifying worldwide revenue is at or above the specified threshold.

315. Subsection (2) details the factors taken into account when determining the fee payable by a regulated service provider. OFCOM will set the fee payable by a provider taking into account the qualifying worldwide revenue for the charging year and any other factors deemed appropriate.

316. Subsection (3) clarifies that in the event of a disagreement between OFCOM and the provider, OFCOM shall determine the fee (or instalment) payable and/or the qualifying worldwide revenue attributable to the relevant period.

317. Subsection (4) references the requirement for OFCOM to determine the fees payable in line with their Statement of Charging Principles: see clause 55.

318. Subsection (5) clarifies that, should a provider only be in scope for part of the charging year, OFCOM has the power to refund all or part of the fee paid by that provider.

319. Subsection (6) is self-explanatory and states that "charging year'', ''fee-paying year'', "qualifying period'', and "qualifying worldwide revenue'' have the same meaning as under clause 51.

Clause 53: Threshold figure

320. This clause details the process to be followed when determining the threshold at, or above which, providers will be required to notify and pay an annual fee (see clauses 51 and 52).

321. Subsection (1) specifies that OFCOM must determine the appropriate threshold figure. First, OFCOM must propose a figure to the Secretary of State: see subsection (2).

322. Then, the Secretary of State must decide whether or not to approve the proposed threshold figure put forward by OFCOM: see subsection (3).

323. If the Secretary of State approves the threshold figure for fees, they must inform OFCOM and OFCOM must then publish the threshold figure: see subsection (3). If the Secretary of State does not approve the threshold figure for fees, they must inform OFCOM and then the Secretary of State must determine, and subsequently publish, a threshold figure that they consider appropriate: see subsection (4).

324. Subsection (5) requires OFCOM to keep the threshold figure under review. If OFCOM considers that the figure should be amended, the steps set out under subsections (1)-(4) of this clause will need to be undertaken again.

325. Subsection (6) requires the first threshold figure to be published prior to the start of the initial charging year when fees become payable.

326. Subsection (7) defines “initial charging year”.

Clause 54: Secretary of State’s guidance

327. This clause sets out the requirement for the Secretary of State to issue guidance relating to fees and the threshold.

328. Subsection (1) references the requirement for the Secretary of State to issue guidance to OFCOM setting out principles to be considered when determining fees payable under clause 52. The guidance must also set out the principles to be considered by OFCOM when determining the threshold figure under clause 53. The Secretary of State must lay the guidance before Parliament (see subsection (4)) and publish it: see subsection (5).

329. Before issuing, revising or replacing the fees and threshold guidance, the Secretary of State must consult OFCOM: see subsection (2). The guidance may not be revised or replaced more frequently than once every three years unless this is agreed by the Secretary of State and OFCOM or it needs to be corrected as a result of subsequent changes to the fee provisions in the Bill: subsection (3).

330. Subsection (6) states that OFCOM is required to have regard to the fees guidance when exercising its functions relating to fees under this Chapter.

Clause 55: Fees statements by OFCOM

331. This clause details the process for OFCOM to publish a Statement of Charging Principles. This clause covers the information that should be included in the Statement, how OFCOM must make or amend the Statement, and how OFCOM should make interested persons aware of the Statement.

332. Subsection (1) requires OFCOM to publish a Statement of Charging Principles outlining the principles which OFCOM will adhere to when setting the fees payable. Without publication of this document OFCOM is not permitted to require providers to pay a fee.

333. Subsection (2) sets out the content of OFCOM’s Statement of Charging Principles. This Statement must outline how the fees charged by OFCOM will meet, but not exceed, the costs of carrying out online safety functions. It must also set out how the fees to be charged to providers are proportionate and justifiable and that there is transparency in relation to the costs incurred and fees charged.

334. Subsection (3) outlines a requirement for the Statement of Charging Principles to include detail on how fees payable under clause 52 are calculated.

335. Subsection (4) sets out a requirement for OFCOM to consult those likely to be affected by the Statement of Charging Principles prior to making or revising the Statement. Those likely to be consulted will include providers with services in scope of the framework.

336. Subsection (5) sets out the requirement for OFCOM to bring the Statement of Charging Principles to the attention of those likely to be affected by it by publishing the Statement in such a way as it considers appropriate.

337. Subsection (6) explains that after the end of each charging year, OFCOM must publish a document which sets out: the total amounts of the fees payable that were received by OFCOM; the total amount of fees that remain outstanding; and OFCOM's total costs of carrying out its online safety functions.

338. Subsection (7) sets out the requirement for any deficit or surplus identified under subsection (6) to be carried forward and taken into account when determining the fees payable for the following year.

339. Subsection (8) clarifies that "OFCOM's costs" include costs incurred by OFCOM in preparing to carry out their online safety functions during a charging year. Subsection (8)(b) clarifies that "OFCOM's costs" also include preparatory costs incurred after clause 55 comes into force but before the initial charging year. Those costs incurred when preparing to carry out the online safety functions, after clause 55 comes into force, should be treated as if they were incurred in the initial charging year.

340. Subsection (9) states that "charging year" has the same meaning as that in clause 51.

Part 4: OFCOM'S Powers and Duties in Relation to Regulated Services

Chapter 1: General Duties

Clause 56: General duties of OFCOM under section 3 of the Communications Act 2003

341. This clause amends OFCOM's existing general duties under section 3 of the Communications Act 2003 (CA 2003), by modifying the list of matters which OFCOM is required to have regard to in carrying out its online safety functions, in order to accommodate OFCOM's new role within the online safety legislative framework.

342. Subsection (2) amends subsection (2) of section 3 of the CA 2003 to provide that, in the carrying out of its functions in relation to regulated services under this Bill, OFCOM is also required to secure the appropriate use, by providers of regulated user-to-user and search services, of systems and processes that protect citizens from harm arising from these services.

343. Subsection (3) amends subsection (4) of section 3 of the CA 2003 so that OFCOM does not need to have regard to the desirability of promoting and facilitating the development of self-regulation in carrying out its functions under this Bill. OFCOM must nonetheless continue to have regard to the other factors in section 3(4) of the CA 2003 in carrying out its online safety functions.

344. Subsection (4) adds subsection (4A) into section 3 of the CA 2003. Section 3(4A) lists the factors that OFCOM must have regard to in performing its duty to further the interests of citizens in online safety matters, so long as OFCOM considers the factor to be relevant.

345. Subsection (5) introduces subsection (5A) into section 3 of the CA 2003 which, as noted above, provides that OFCOM does not need to have regard to the desirability of promoting and facilitating the development of self-regulation in carrying out its online safety functions.

346. Subsection (6) introduces subsection (6ZA) into section 3 of the CA 2003. This new subsection will make it clear that, where OFCOM's duties under this Bill conflict with its duty under section 24 of the CA 2003 to provide information to the Secretary of State to secure compliance with an international obligation, OFCOM's duty under section 24 will take priority.

347. Subsection (8) introduces new subsection (15) into section 3 of the CA 2003 to provide that the terms 'content', 'harm', 'provider' and 'regulated service' have the same meaning as in this Bill.

348. Subsection (9) also relates to self-regulation and amends section 6 of the CA 2003 to ensure online safety functions are not subject to OFCOM's duty to consider whether or not their general duties, set out in section 3, may be furthered or secured, or are likely to be furthered or secured, by effective self-regulation.

Clause 57: Duties of OFCOM in relation to strategic priorities

349. This clause sets out OFCOM's duties in relation to statements of strategic priorities designated by the Secretary of State under clause 109. For further information on statements of strategic priorities, see clause 109.

350. Subsection (2) provides that OFCOM must have regard to the statement of strategic priorities when carrying out relevant statutory functions relating to online safety.

351. Subsection (3) specifies that within 40 days of the statement being issued, or within a longer period if the Secretary of State allows, OFCOM must explain in a written, published statement what it proposes to do as a result of the statement of strategic priorities when exercising its regulatory functions.

352. Subsection (4) states that after the statement of strategic priorities is designated, OFCOM must publish an annual review of what it has done with regard to the strategic priorities outlined in it.

Clause 58: Duty to carry out impact assessments

353. This clause extends OFCOM's duty to carry out impact assessments on important proposals under section 7 of the Communications Act 2003 (CA 2003) to the online safety sphere, with modifications to accommodate the exercise of the duty in the online safety context.

354. Subsection (3) introduces subsection (2A) into section 7 of the CA 2003. Section 7(2A) of the CA 2003 will provide that all proposals to introduce, replace or amend codes of practice under this Bill are "important proposals" for the purposes of OFCOM's duty to carry out impact assessments. This means that OFCOM will (subject to urgency considerations) either need to undertake and publish an impact assessment on these proposals, or to publish a statement detailing why they consider such an assessment unnecessary.

355. Subsection (4) introduces subsections (4A) and (4B) into section 7 of the CA 2003. Section 7(4A) of the CA 2003 will provide that all assessments of proposals mentioned in subsection (2A) must include an assessment of the likely impact of implementing the proposal on small and micro businesses. Section 7(4B) of the CA 2003 will provide that all assessments of proposals which relate to the carrying out of OFCOM's online safety functions must include an assessment of the likely impact of implementing the proposal on small and micro businesses. If only part of the proposal relates to OFCOM's online safety functions, then only that part must be assessed to determine its likely impact on small and micro businesses.

Chapter 2: Register of Categories of Services

Clause 59 and Schedule 4: Register of categories of services

356. The Bill creates different categories of regulated services which will be subject to additional duties. This clause imposes a duty on OFCOM to establish a register of these particular categories of regulated services with one part for each of the following:

a. user-to-user services meeting the Category 1 threshold conditions;

b. search services meeting the Category 2A threshold conditions;

c. user-to-user services meeting the Category 2B threshold conditions.

357. The threshold conditions are to be specified in regulations made by the Secretary of State. Once the relevant regulations have been made, under paragraphs (b) to (e) of subsection (1), OFCOM will be required to assess whether each regulated service which it considers is likely to meet either the Category 1, Category 2A or Category 2B threshold conditions does in fact meets those threshold conditions and, if it does, to add it to the relevant part of the register.

358. The additional duties placed on providers of Category 1, Category 2A and Category 2B services are established elsewhere in the Bill but can be summarised as follows:

a. Category 1 (see clause 5(5) and clause 49): Duties with regard to content that is harmful to adults, duties to protect content of democratic importance and journalistic content, additional reporting and redress duties and additional duties with regard to protecting users' freedom of expression and privacy rights. Category 1 services will also have a duty to produce annual transparency reports.

b. Category 2A and 2B (see clause 49): A duty to produce annual transparency reports. Such reports may include, for example, information about the measures service providers are taking to counter illegal content or activity on their services.

359. Subsection (2) provides details on what each part of the register should contain, specifically the name and a description of each regulated service that, in OFCOM's opinion, meets the relevant threshold conditions, and the name of the provider of each of those services.

360. Subsection (3) provides that, should a regulated user-to-user service meet both the Category 1 and Category 2B threshold conditions, it should only be added to the Category 1 part of the register.

361. Subsection (4) makes clear that OFCOM must make reasonable efforts to obtain or generate information or evidence for the purposes of assessing a service against the threshold conditions. Subsection (5) requires OFCOM to publish the register in whatever manner it considers appropriate for bringing it to the attention of persons who, in its opinion, are likely to be affected by it.

362. Subsection (6) makes clear that a service becomes a Category 1, Category 2A or Category 2B service by virtue of being included in the relevant part of the

register. This means that the provider of a regulated service has additional duties in respect of that service once the service is included on the published register.

363. Schedule 4 requires the Secretary of State to make regulations to specify the threshold conditions that a regulated service must meet to be included in the relevant part of the register and makes associated provision about advice from OFCOM: see clause 59(7).

364. Subsection (8) provides that the terms “Category 1 threshold conditions”, “Category 2A threshold conditions”, and “Category 2B threshold conditions” have the same meaning in this clause as they do in Schedule 4.

Schedule 4

365. Paragraph 1 (1), (2) and (3) require the Secretary of State to make regulations setting threshold conditions for Category 1, Category 2A and Category 2B services; that is the conditions which a relevant service must meet in order to be designated as a Category 1, Category 2A or Category 2B service.

366. Paragraph 1(4) provides that regulations under sub-paragraphs (1), (2) and (3) must specify how a service may meet the relevant threshold conditions. For user-to-user services, at least one threshold condition about number of users and at least one threshold condition about functionality must be met in order for the service to be designated as a Category 1 or a Category 2B service and, for search services, at least one threshold condition about number of users must be met for the service to be designated as a Category 2A service. Therefore, a user-to-user service assessed as meeting a Category 1 threshold condition related to the number of users but not meeting any Category 1 conditions related to functionality would not be designated as a Category 1 service.

367. For Category 1 services, paragraph 1(1) provides that such conditions must only relate to a regulated user-to-user service’s number of users (paragraph 5 makes it clear that this means the number of UK users) and its functionalities.

In making regulations which set these Category 1 threshold conditions, paragraph 1(5) provides that the Secretary of State must consider how the number of users of a service and the service’s functionalities will likely affect the risk of harm to adults from content which is harmful to adults being spread via the service. This requirement to consider the impact on the risk of harm to adults reflects the fact that providers of Category 1 services owe additional safety duties on the services in question in relation to content which is harmful to adults.

368. For Category 2A services, threshold conditions must relate to a regulated search service’s number of users (paragraph 5 makes it clear that this means the number of UK users) and any other factors that the Secretary of State considers relevant. (Note that there is no requirement for the Secretary of State to specify a condition relating to the service’s functionalities.) Paragraph 1(6) makes it clear that, in making regulations which set these threshold conditions, the Secretary of State must consider how the number of users will likely affect the risk of harm to individuals

from illegal content or content which is harmful to children which may be encountered in or via search results.

369. For Category 2B services, threshold conditions must relate to a regulated user-to-user service's number of users (paragraph 5 makes it clear that this means the number of UK users) and its functionalities, and any other factors that the Secretary of State considers relevant. Paragraph 1(7) makes it clear that, in making regulations which set these threshold conditions, the Secretary of State must consider how the number of users and a service's functionalities will likely affect the risk of harm to individuals from illegal content or content which is harmful to children or adults which may be encountered via the service.

370. Paragraph 2 establishes the procedure for the making of the first set of regulations under paragraph 1. Sub-paragraphs (2), (3) and (4) of paragraph 2 set out that OFCOM must carry out research to inform the making of these regulations.

a. For Category 1 services, paragraph 2(2) states that OFCOM's research must consider the relationship between (on the one hand) the dissemination of content that is harmful to adults on regulated user-to-user services and (on the other) the number of users and functionalities of such services. This reflects the fact that providers of Category 1 services owe additional safety duties in relation to content which is harmful to adults in respect of those services.

b. For Category 2A services, paragraph 2(3) provides that OFCOM's research must consider the prevalence of illegal content and content which is harmful to children presented to users in response to searches made by users using regulated search services; and (on the other) the number of users of such services; and any other factors OFCOM considers relevant.

c. For Category 2B services, paragraph 2(4) provides that OFCOM's research must consider the spreading of illegal content, content that is harmful to children and content that is harmful to adults via regulated user-to-user services; and (on the other) the number of users and functionalities of such services; and any other factors OFCOM considers relevant.

371. The research must be carried out within six months of Royal Assent. However, for research in relation to Category 2A and 2B services, paragraph 2(10) allows for the Secretary of State to give OFCOM extra time to carry out the research, up to a limit of 18 months after Royal Assent.

372. OFCOM must then provide advice to the Secretary of State, based on its research, as to what it thinks would be appropriate threshold conditions for the regulations to make (paragraph 2(5) of Schedule 4). In respect of Category 2A and 2B threshold conditions, such advice may include advice that the regulations should include another factor in addition to number of users (and, for user-to-user services, functionalities), and what that other factor should be.

373. Paragraph 2(7) states that, as soon as reasonably practicable after OFCOM has provided its advice, OFCOM must publish this advice and the Secretary of State

must make the regulations. Paragraph 2(11) provides that the Secretary of State cannot make regulations setting threshold conditions until OFCOM has carried out its research and provided advice to the Secretary of State. In publishing its advice, paragraph 4 provides that OFCOM must have regard to the need to exclude confidential matters (as defined in sub-paragraphs (2) and (3) of paragraph 4) from publication as far as practicable, and that OFCOM must publish its advice in the manner it considers appropriate.

374. If the regulations include provision which differs in any material respect from what was advised by OFCOM, the Secretary of State must publish a statement explaining why they have departed from that advice (paragraph 2(8) of Schedule 4). The publication of such a statement must happen before or at the time of making the regulations and in such a manner that the Secretary of State believes is appropriate for bringing it to the attention of persons who may be affected by it.

375. After the regulations are made, OFCOM will be required to assess services which it considers are likely to meet the relevant threshold conditions against the threshold conditions set out in the regulations, and to establish a register of Category 1, Category 2A and Category 2B services (see clause 59(1)). Services become subject to Category 1, 2A or 2B duties by virtue of being added to the relevant part of the register.

376. Paragraph 3 establishes the procedure for updating the threshold conditions by amending or replacing regulations made under paragraph 1. Paragraphs 3(1), (2) and (3) state that, for Category 1, Category 2A and Category 2B conditions respectively, regulations may only be amended or replaced by further regulations, once OFCOM has carried out further research. The research must consider the same topics as set out in Paragraphs 2(2), (3) and (4). Paragraph 3(12) states, however, that such further research is not required where regulations are being made only for the purpose of correcting existing regulations that were made under paragraph 1.

377. Paragraph 3(4) states that either OFCOM or the Secretary of State may initiate the carrying out of this further research and the research should be carried out to the depth that OFCOM considers appropriate. This ensures that OFCOM is only required to carry out research insofar as it is proportionate to changes in the areas which it is researching. If the further research is initiated by a request from the Secretary of State, paragraph 3(5) provides that the request must state why the Secretary of State considers further research to be necessary.

378. Paragraph 3(6) states that following further research being carried out, OFCOM must advise the Secretary of State whether or not, in OFCOM's opinion, changes to the regulations are appropriate (and if it does consider changes appropriate, what those changes should be). Paragraph 3(7) notes that OFCOM must publish this advice as soon as reasonably practicable after providing it. In publishing its advice, paragraph 4 provides that OFCOM must have regard to the need to exclude confidential matters (as defined in sub-paragraphs (2) and (3) of paragraph 4) from publication as far as practicable, and that OFCOM must publish its advice in the manner it considers appropriate.

379. Paragraphs 3(8) and (9) impose duties on the Secretary of State, if they take action which departs from OFCOM's advice. If OFCOM advises the Secretary of State to amend or replace the regulations, and the Secretary of State does so in line with OFCOM's advice, no specific action is needed beyond amending or replacing the Regulations. However, in any of the following situations, the Secretary of State must publish a statement explaining their decision:

a. If OFCOM advises the Secretary of State to amend or replace the Regulations, and the Secretary of State amends or replaces the regulations, in a way that differs in any material respect from OFCOM's advice.

b. If OFCOM advises the Secretary of State not to amend or replace the Regulations, but the Secretary of State chooses to replace or amend the Regulations.

c. If OFCOM advises the Secretary of State to amend or replace the Regulations, but the Secretary of State chooses not to replace or amend the Regulations.

380. In situations (a) and (b) the statement must, by virtue of paragraphs 3(10) and 3(11), be published before or at the time at which the regulations to which it relates are made and in such a manner as the Secretary of State considers appropriate for bringing it to the attention of persons who may be affected by it. In situation (c), the statement must, by virtue of paragraphs 3(9) and 3(11), be published as soon as reasonably practicable and also in such a manner as the Secretary of State considers appropriate for bringing it to the attention of persons who may be affected by it.

381. Throughout this Schedule, references to the number of users of a service are to the number of users of a service who are in the United Kingdom (Paragraph 5). "User" is defined in clause 122, and includes entities, as well as non-registered users of services. Paragraph 6 further notes that the meanings of the terms "illegal content", "content that is harmful to children" and "content that is harmful to adults" are as found in clause 41, clause 45 and clause 46 respectively.

Clause 60: OFCOM's duty to maintain register

382. This clause sets out OFCOM's duties with regards to maintaining the register of regulated services that are designated as either Category 1, Category 2A or Category 2B. Further detail on the register is set out in clause 59.

383. Subsections (1), (2) and (3) state that, for Category 1, Category 2A and Category 2B services respectively, if regulations setting threshold conditions are amended or replaced, OFCOM must conduct a full reassessment of services which it considers are likely to meet the amended thresholds set in the relevant regulations. It must then update the register accordingly. OFCOM must do this as soon as is reasonably practicable after the date on which the amending or replacement regulations are made.

384. At any other time, subsection (4) requires OFCOM to assess services which are not on the register, but which it considers are likely to meet the threshold conditions for designation as a Category 1, Category 2A or Category 2B service, and to add them to the relevant part of the register accordingly if they are assessed to meet the threshold conditions. In practice, this allows OFCOM to respond to changes relating to a regulated service and to ensure that the register remains up-to-date. For example, the size of a service's audience may grow rapidly, and/or the functionalities present on the service may be added to. Should it therefore believe that the service is now likely to meet the Category 1, Category 2A or Category 2B threshold conditions, OFCOM would be obliged to assess the service and, if it does in fact meet the relevant threshold conditions, to add it to that part of the register.

385. Subsections (5) to (7) allow providers of a service listed in the register to request the service's removal from the register. If they make such a request, OFCOM must first determine whether it is satisfied, based on the evidence submitted by the provider in question, that there has been a change to the service which appears likely to be relevant. Only if OFCOM is satisfied that there has been a change which appears likely to be relevant is OFCOM obliged to assess the service and notify the provider of its decision. This ensures that OFCOM does not have to do a full assessment every time a request is made, which could create disproportionate burdens, but that requests which stem from a genuine change in circumstances will still receive full consideration. If OFCOM assesses the service to no longer meet the relevant thresholds, OFCOM must remove it from the relevant part of the register.

386. Subsection (8) requires OFCOM to take reasonable steps to obtain or generate information or evidence to inform its assessments of services under this clause, in the same way as it is required to do for the original assessments undertaken when the register is first established.

387. Subsection (9) requires OFCOM to re-publish the register each time a change is made to it.

388. Subsection (10) refers to the appeals section of the Bill, for provisions about appeals against a decision to either include a service in the register, or a decision not to remove a service from the register.

389. Subsection (11) defines the terms 'register' and 'registration day' and subsection (12) states that the terms "Category 1 threshold conditions", "Category 2A threshold conditions", and "Category 2B threshold conditions" have the same meaning in this clause as they do in Schedule 4.

Chapter 3: Risk assessments

Clause 61: Risk assessments by OFCOM

390. This clause places a duty on OFCOM to carry out risk assessments to identify, assess and understand the risks of harm to individuals in the UK presented by regulated services. It sets out the steps that OFCOM must take to fulfil this duty.

This includes requirements to develop a risk profile for different kinds of regulated services and to publish risk assessments and keep them up to date.

391. Subsection (2) specifies that the risk assessment must, amongst other things, assess the levels of risk of harm presented by regulated services of different kinds. It sets out the areas that must be considered when assessing the risk of harm.

392. Subsection (3) sets out that OFCOM must develop risk profiles for different kinds of regulated services. OFCOM should categorise these services as it considers appropriate. This must take into account the services' characteristics, which include user base, business model, governance and other systems and processes (see subsection (6)), the risk levels, and any other relevant matters identified in its risk assessment.

393. Subsection (4) requires OFCOM to publish a report on its findings, and OFCOM must ensure that the risk assessment is kept up to date (subsection (5)).

Clause 62: OFCOM's guidance about risk assessments

394. This clause places a duty on OFCOM to produce guidance for providers of regulated services to assist them in complying with their duties under clauses 7 and 19 (risk assessment duties for user-to-user services and search services respectively). Subsection (1) sets out that OFCOM must prepare this guidance as soon as reasonably practicable.

395. Subsection (2) requires the guidance to include the risk profiles prepared under clause 61. These risk profiles will categorise the services as OFCOM consider appropriate, taking into account the characteristics of the services and the risk levels and other matters identified in the risk assessment

396. OFCOM must also keep the guidance up-to-date and publish it - including any revised or replacement guidance: see subsections (3) and (4).

Chapter 4: Use of technology in relation to terrorism content and child sexual exploitation and abuse content

Clause 63: Use of Technology Warning Notice

397. Chapter 4 provides the statutory basis for OFCOM's power to require a service provider to use accredited technology to identify and remove terrorist content on public channels and child sexual exploitation and abuse (CSEA) content on private and public channels.

398. Subsection (1) of this clause sets out that if OFCOM has reasonable grounds for believing that the provider of a user to user service or search service is failing to comply with the duty in section 9 (safety duties about illegal content) so far as the duty relates to terrorism and CSEA content, OFCOM may issue a Use of Technology Warning Notice. The purpose of the Warning Notice is to provide the service provider with notice that OFCOM is considering requiring it to use the technology that is specified in the notice.

399. Subsection (2) sets out that if OFCOM has reasonable grounds for believing that the provider of a regulated user-to-user service is failing to comply with the duty in section 9 (safety duties about illegal content), so far as relating to terrorism content or CSEA content (or both those kinds of content), based on evidence demonstrating — (a) the prevalence, and (b) the persistent presence, of terrorism content or CSEA content or both on the service in question, it may issue a Use of Technology Warning Notice.

400. Subsection (3) sets out that if OFCOM has reasonable grounds for believing that the provider of a regulated search service is failing to comply with the duty in section 21 (safety duties about illegal content), so far as relating to terrorism content or CSEA content (or both those kinds of content), based on evidence demonstrating — (a) the prevalence, and (b) the persistent presence, of terrorism content or CSEA content or both on the service in question, it may issue a Use of Technology Warning Notice.

401. Subsection (4) sets out the information contained within the Warning Notice. These include OFCOM's reasons for issuing the Notice and the type of technology the service provider would be required to use.

402. Subsection (5) provides that the service provider in question will have the opportunity to make representations to OFCOM over a given period, before OFCOM decide whether to issue a Use of Technology Notice. OFCOM may decide not to issue a Use of Technology Notice and take no further action.

Clause 64: Use of Technology Notice: user-to-user service

403. This clause sets out the circumstances under which OFCOM may issue a Use of Technology Notice to a provider of a regulated user-to-user service, and the conditions that must be met before the power can be used.

404. Subsection (1) clarifies when OFCOM may issue a Use of Technology Notice to the service provider. A Use of Technology Warning Notice (under clause 63) must have already been issued to a provider of a regulated user-to-user service, and then the period for written representations under clause 63(5)(b) must have passed.

405. Subsection (2) sets out that OFCOM may decide not to issue the provider with a Use of Technology Notice after considering representations from the provider, or further evidence. OFCOM must notify the provider of its decision.

406. Subsection (4) states that OFCOM may require a service provider to use accredited technology to identify public terrorism content included in the service (as defined in subsection (10)) and/or child sexual exploitation and abuse (CSEA) content included in any part of the service. The service must take down that content swiftly. The requirements will be set out in a Use of Technology Notice.

407. Subsection 5 (a) - (c) set out the conditions that must be satisfied before OFCOM can issue a Use of Technology Notice. The conditions are that: OFCOM must have evidence of persistent and prevalent terrorism and/or CSEA content; OFCOM must have concluded that any alternative, and less intrusive measures,

would not effectively address the problem; OFCOM's intervention must be a proportionate means of addressing the problem.

408. Subsection (6) provides that where a service provider is already using technology on a voluntary basis, but this is ineffective, OFCOM can still intervene and require a service provider to use a more effective technology, or the same technology in a more effective way.

409. Subsection (7) specifies that OFCOM can include in the notice a requirement to operate an effective procedure for users to challenge the removal of their content from the service.

410. Subsection (8) defines public terrorism content.

411. Subsection (9) states that OFCOM may vary or revoke a Use of Technology Notice by issuing a further notice under this section.

Clause 65: Use of Technology Notice: search service

412. This clause sets out the circumstances under which OFCOM may issue a Use of Technology Notice to a regulated search service, and the conditions that must be met before the power can be used.

413. Subsection (1) clarifies when OFCOM may issue a Use of Technology notice to the service provider. A Use of Technology Warning Notice (under clause 63) must have already been issued to a provider of a regulated search service, and the period for written representations under clause 63 (5)(b) must have passed.

414. Subsection (2) sets out that OFCOM may decide not to issue the provider with a Use of Technology Notice after considering representations from the provider, or further evidence. OFCOM must notify the provider of its decision.

415. Subsection (4) states that OFCOM may require a service provider to use accredited technology to identify public terrorism and/or child sexual exploitation and abuse (CSEA) content included in the search results of a service. The service must take steps to prevent that content appearing in search results swiftly. The requirements will be set out in a Use of Technology Notice.

416. Subsection 5 (a) - (c) set out the conditions that must be satisfied before OFCOM can issue a Use of Technology Notice. The conditions are that: OFCOM must have evidence of persistent and prevalent terrorism and/or CSEA content in the search results of that service; OFCOM must have concluded that any alternative, and less intrusive measures, would not effectively address the problem; OFCOM's intervention must be a proportionate means of addressing the problem.

417. Subsection (6) provides that where a service provider is already using technology on a voluntary basis, but this is ineffective, OFCOM can still intervene and require a service provider to use the same technology in a more effective way.

418. Subsection (7) specifies that OFCOM can include in the notice a requirement to operate an effective procedure for users to challenge the removal of their content from the service.

419. Subsection (8) provides that OFCOM may vary or revoke a notice by issuing a further notice under this same section.

Clause 66: Use of Technology Notices: supplementary

420. Subsection (1) sets out the statutory requirements for the information that must be included in the Use of Technology Notice. These do not need to be exactly the same as the warning notice because OFCOM may have considered representations from the service provider.

421. Subsection (2) sets out that OFCOM can initially issue a Use of Technology Notice imposing requirements for up to 36 months from the point of implementation.

422. Subsection (3) states that a Use of Technology Notice may only require a regulated provider to use accredited technology in relation to regulated services in the UK or regulated services that affect users in the UK.

423. Subsections (4) and (5) explain that OFCOM will only be able to require the use of tools that meet the minimum standards for accuracy for detecting terrorism and/or CSEA content as set out by the Secretary of State. Any tools that OFCOM requires the use of must have been accredited by either OFCOM or a delegated third party as meeting these minimum standards.

424. Subsection (6) states that within this section, Use of Technology Notice means the same as in clauses 64 and 65.

Clause 67: Further Use of Technology notice

425. Subsection (1) sets out that this clause applies where OFCOM has given a Use of Technology Notice under clause 64 or 65.

426. Subsection (2) sets out that if there are reasonable grounds for believing that the provider is failing to comply with the Use of Technology Notice, and the conditions, as set out in clause 64(5) or 65(5) are still met, OFCOM can revoke the notice at any time and issue the provider a Further Use of Technology Notice. This may be in parallel with enforcement measures against the breach of the original notice.

427. Subsection (3) requires OFCOM to review the use of the specified technology within 36 months of the date set by OFCOM in the original notice. Subsection (4) specifies what OFCOM must consider in its review.

428. Subsection (5) specifies that following the review, and after consultation with the provider, OFCOM may give the provider a Further Use of Technology Notice if OFCOM reasonably consider that there is a significant risk that, without the continued use of accredited technology, terrorism content or child sexual exploitation and abuse (CSEA) content (or both) will become prevalent, and persistently present,

on the service. Under subsection (6) the conditions set out in Subsections (2)-(5) apply again.

429. Subsection (7) allows a Further Use of Technology Notice to require the use of different accredited technology from an earlier Use of Technology Notice.

430. Subsection (8) notes that Subsections (4) and (6) to (9) of clause 64, and clause 66, apply in relation to a Further Use of Technology Notice to a user-to-user service under this section as they apply in relation to a Use of Technology Notice under those section(s).

431. Subsection (9) notes that Subsections (4) and (6) to (8) of clause 65, and clause 66, apply in relation to a Further Use of Technology Notice to a search service under this section as they apply in relation to a Use of Technology Notice under those clauses(s).

Clause 68: Guidance about requiring use of technology

432. This clause requires OFCOM to issue guidance setting out the circumstances under which it could require a service provider in scope of the power to use technology to identify CSEA and/or terrorism.

433. OFCOM will have the discretion to decide on the exact content of the guidance and must keep it under review and publish it. OFCOM must also have regard to its guidance when exercising these powers.

Clause 69: Annual report about use of technology

434. This clause requires OFCOM to report annually to the Secretary of State, on the exercise of its power during the last year and on current and in-development technology that is likely to meet the required minimum standards of accuracy.

435. Subsection (2) says that the Secretary of State must lay this report before Parliament.

436. Subsection (3) cross-refers to section 102 which sets out provisions for OFCOM excluding confidential information from its published reports.

Chapter 5: Information

Information power

Clause 70: Power to require information

437. Subsection (1) gives OFCOM the power to require a person to provide it with information which it requires for the purpose of exercising (or deciding to exercise) any of its online safety functions. This information must be requested by an "information notice" and this clause also provides for what must be stipulated in an information notice and imposes duties on the recipients of such notices. Subsection (6) states that the information required by OFCOM can include information held in any form, including electronic form.

438. Subsection (2) states that OFCOM is only able to require a person to provide information if it believes that the person it is asking for the information is either able to generate or obtain that information.

439. Subsection (3) lists the types of persons OFCOM can require information from. This includes regulated providers and people providing ancillary services (including entities which might be required to implement business disruption measures, e.g. internet access services and application stores).

440. Subsection (4) sets out a non-exhaustive list of reasons why OFCOM might need to require information using the power specified in subsection (1), such as assessing compliance with any of the safety duties. For example, OFCOM could require a provider of a regulated service to explain the potential risks associated with the operation of their algorithms and recommendation tools and what measures they had put in place to mitigate these risks, in order to help determine whether the provider was fulfilling the duty of care.

441. Subsection (5) refers to clause 71, which allows OFCOM to require a provider of a regulated service to name a senior manager in its response to an information notice.

442. Subsection (7) states that when OFCOM requires the production of documents, they can take copies of those documents, or extracts from them. OFCOM can also require that the person producing a document explain its contents.

443. Subsection (8) states what should be specified within an information notice, including the information to be provided, why OFCOM requires it, where and in what format it should be provided, and information on the consequences of non-compliance with the information notice.

444. Subsection (9) states that an information notice must specify a deadline for when the information must be provided. This deadline could entail that the information is required by a specific date, within a specific period, or at specified intervals (e.g. quarterly).

445. Subsection (10) states that the person who has been given an information notice has a duty to comply with the requirements stated in that notice, and to ensure all the information they provide is accurate.

446. Subsection (11) states that OFCOM may cancel an information notice by sending a notice to the original recipient.

447. Subsection (12) states that the power in subsection (1) cannot be used where legal professional privilege (or, in Scotland, confidentiality of communications) would be compromised.

448. Subsection (13) clarifies the meaning of the term “provider of a regulated service” and states that this includes former providers of a regulated service.

449. Subsection (14) clarifies the meaning of the terms “information” and “officer”. For “information”, it is stated that this includes documents and any reference to

providing information also encompasses producing a document. For “officer”, it is stated that this includes a director, a manager, a secretary or, where the affairs of the entity are managed by its members, a member.

450. Subsection (15) states that for information that is not recorded in a legible form, references to producing a document are to produce a copy of the information in legible form.

Clause 71: Requirement to name a senior manager

451. OFCOM may pursue criminal action against a named senior manager of a provider of a regulated service that fails to comply with an information notice (as per clause 73 described below). This clause provides OFCOM with the power to require an entity to name the relevant senior manager.

452. Subsection (2) gives OFCOM the power to include in its information notice a requirement for the provider of a regulated service to name an individual who is considered to be a senior manager of the entity.

453. Subsection (3) requires OFCOM to set out, in its information notice, that the provider must inform that person that they have been named, and also set out the consequences for such an individual of the entity not complying with the information notice.

454. Subsection (4) defines a senior manager as an individual who plays a significant role in making decisions about the managing and organising of the entity’s “relevant activities” and also in the actual managing or organising of such activities. Subsection (5) defines “relevant activities” as activities relating to the entity’s compliance with the regulatory requirements imposed by this Bill in connection with the regulated service to which the information notice relates.

Information offences

Clause 72: Offences in connection with information notices

455. Criminal proceedings may be brought against a provider of a regulated service in connection with information notices. This clause sets out the criminal offences that can be committed by a provider of a regulated service.

456. Subsection (2) states that a provider commits an offence if it fails to comply with an information notice. Subsection (3) sets out that it is a defence if a provider of a regulated service can show that it was not reasonably practicable to comply with the information notice but they have subsequently taken all reasonable steps to do so.

457. Subsection (4) states that a provider commits an offence if it provides or publishes materially false information in response to an information notice and either knows it is false or is reckless as to whether it is false.

458. Subsection (5) states that a provider commits an offence if it provides or publishes encrypted information that is not possible for OFCOM to understand, and that their intention was to prevent OFCOM from understanding such information.

459. Subsection (6) establishes that the offence is triable either way and sets out the maximum sentences that can be imposed by the relevant criminal court on conviction for this offence.

Clause 73: Senior managers' liability: information offences

460. Criminal action may be brought against a senior manager of a provider of a regulated service if that provider has failed to comply with an information notice, and the individual has been named as the senior manager by the provider in accordance with clause 71 above. This clause sets out the criminal offence that can be committed by the relevant named senior manager.

461. Subsection (2) states that a named senior manager commits an offence if it is found that the provider itself committed the offence under clause 72 (failure to comply with an information notice) and the named senior manager failed to take all reasonable steps to prevent that offence being committed.

462. Subsection (3) sets out that it is a defence if the named senior manager can show that they were not a senior manager (within the definition of clause 71(4)) during the period (i) starting from the date of the information notice and (ii) ending four weeks after the date by which the provider was required to comply with the information notice (and submit the information to OFCOM).

463. Subsection (4) states that a named senior manager commits an offence if the entity commits the offence of providing false information to OFCOM (as per clause 72(4)) and the named senior manager fails to take all reasonable steps to prevent that offence being committed.

464. Subsection (5) states that a named senior manager commits an offence if the entity commits the encrypted information offence as per clause 72(5) and the named senior manager fails to take all reasonable steps to prevent that offence being committed.

465. Subsection (6) states that it is also a defence for the individual charged with the offences under subsections (4) or (5) to show that they were not a senior manager within the meaning under clause 71 at the time at which the act constituting the offence was committed.

466. Subsection (7) states that it is a defence for an individual charged with an offence under this clause to show that they had no knowledge of being named as a senior manager in a response to the information response in question.

467. Subsection (8) establishes that the offence is triable either way and sets out the maximum sentences that can be imposed by the relevant criminal court on conviction.

Skilled persons' reports

Clause 74: Reports by skilled persons

468. This clause gives OFCOM the power to require a report from a skilled person into a failure, a possible failure or a risk of a failure by a provider of a regulated service to comply with a "relevant requirement" (as listed in subsection (9)).

469. Subsection (1) specifies that OFCOM can use this power if it reasonably believes that it is necessary to do so to:

a. identify and assess a failure or possible failure by a provider of a regulated service to comply with a relevant requirement (subsection (1)(a)); and/or
b. develop its understanding of the risk of a provider of a regulated service failing to comply with a relevant requirement, and of how to mitigate that risk (subsection (1)(b)).

470. Subsection (2) further provides that, in order to exercise its powers for the purpose of subsection (1)(b), OFCOM would need to reasonably believe that the provider may be at risk of failing to comply with a relevant requirement.

471. Subsection (3) sets out that OFCOM may appoint a skilled person to carry out a report into matters relevant to the purpose in subsection (1) for which OFCOM exercised its powers ("the relevant matters"), and notify the provider. Alternatively, as set out in subsection (4), OFCOM can give a notice to the provider requiring them to appoint a skilled person to produce a report for OFCOM, in the form stipulated by OFCOM, and specifying the relevant matters that must be dealt with in the report.

472. Subsection (5) specifies that a skilled person either must be judged by OFCOM to have the skills necessary to carry out the report, or, if the provider is appointing the skilled person, must be a person nominated or approved by OFCOM.

473. Subsection (6) requires the service provider to pay the skilled person's remuneration and expenses relating to the preparation of the report and to pay said remuneration and expenses directly to the skilled person. Subsection (7) further provides that, in the event of non-payment, the amount due to a skilled person is recoverable through the courts.

474. Subsection (8) requires the service provider, anyone who works or has worked for the provider, anyone who is providing or has provided services to the provider related to the relevant matters which form the subject of the report, and other providers of internet services to help the skilled person in any way that they might reasonably need in their preparation of the report.

475. Subsection (9) sets out the relevant requirements. These include a provider's safety duties relating to illegal content, its safety duties to protect adults, its safety duties for services likely to be accessed by children, and its transparency reporting duties.

Investigations and interviews

Clause 75: Investigations by OFCOM

476. This clause relates to investigations by OFCOM into whether a provider of a regulated service has failed, or is failing, to comply with a "relevant requirement".

Subsection (1) requires a provider of a regulated service to cooperate fully with any such investigation.

477. Subsection (2) provides a definition of a "relevant requirement" for these purposes. This encompasses the list of duties and requirements in clause 82 and any requirements imposed by a use of technology notice under section 64, 65 or 67.

Clause 76: Power to require interviews

478. This clause gives OFCOM the power to require an individual to attend an interview. Subsection (1) states that this power can be used when OFCOM is carrying out an investigation into the failure, or possible failure, of a provider of a regulated service to comply with a relevant requirement.

479. Subsection (2) specifies that OFCOM may by notice require an individual to attend an interview and answer questions about any matters relevant to the investigation. This interview can be in person or a remote interview. The notice should specify the period of time within which the individual must attend the interview. Subsection (3) specifies that the notice must also indicate the subject matter and purpose of the interview.

480. Subsection (4) lists the following individuals who can be required to attend an interview:

a. a member or officer of the provider of the regulated service,

b. an employee of the provider, and

c. an individual who was a member, officer, or employee of the provider at a time to which the information required by OFCOM relates.

481. Subsection (5) specifies that this clause does not require a person to disclose information that could be maintained to be legally privileged in legal proceedings (or, in Scotland, to confidentiality of communications).

482. Subsection (6) defines "relevant requirement" as having the meaning given by clause 74 (subsection 9).

Powers of entry and inspection

Clause 77: Powers of entry and inspection

483. This clause gives force to Schedule 5 to the Bill, which makes provision about powers of entry and inspection.

Schedule 5

Authorised persons

484. Schedule 5 sets out OFCOM's powers of entry and inspection. Paragraph (1)(1) states that OFCOM may authorise persons to (i) exercise its powers of entry

and inspection without a warrant under paragraph 2 or (ii) apply for a warrant to be issued under paragraph 3.

485. Paragraph (1)(2) defines “authorised person” as someone authorised to enter and inspect a property either without a warrant or pursuant to a warrant. Subsection (1)(3) specifies that their authorisation must be in writing.

Power of entry and inspection without a warrant

486. Paragraph (2)(1) states that OFCOM’s power of entry and inspection may only be exercised without a warrant if (i) OFCOM believes that the relevant premises are being used by a provider of a regulated service in connection with the provision of the regulated service and (ii) seven days’ notice has been given to the occupier of the premises that OFCOM propose to come and inspect the premises. Sub-paragraph (2) states that the power to enter and inspect must be exercised at a reasonable hour.

487. Sub-paragraph (3) states that, before exercising a power of entry under this paragraph, an authorised person must, if requested to do so, produce evidence of their identity and outline the purpose for which they are seeking to enter the premises.

488. Sub-paragraph (4) lists what an authorised person may do under paragraph (2) This includes entering and inspecting the premises, requiring documents to be produced and requiring any person on the premises to provide an explanation of any document. Paragraph (2)(5) provides that the authorised person may make copies or extracts of documents found.

489. Paragraph (2)(6) states that an authorised person may only exercise a power of entry and inspection under paragraph (2) if the information or document they are seeking to obtain is required in connection with the exercise by OFCOM of its functions under this Bill.

Conditions for issue of a warrant

490. Paragraph (3) deals with the conditions for the issue of a warrant by a justice for the inspection of premises by OFCOM. Sub-paragraph (1) provides that a justice may only issue a warrant in relation to premises specified in an application if they are satisfied on the basis of sworn written evidence that the premises are being used by the provider of a regulated service in connection with the provision of a regulated service. In addition, the justice must be satisfied that there are reasonable grounds to suspect that the provider is failing to comply, or has failed to comply, with enforceable requirements relating to that service (see sub-paragraph (3)) and that there are documents or records on the premises, or documents or records which can be viewed at the premises, or equipment on the premises, relevant to an OFCOM’s investigation into that failure. Furthermore, at least one of the conditions below in sub-paragraph (2) must be satisfied.

491. Sub-paragraph (2) lists further conditions for issuing a warrant, at least one of which must be satisfied in addition to those in sub-paragraph (1). The condition in

paragraph (a) is that OFCOM has given seven days' notice to the occupier of the premises demanding access, but access to the premises at a reasonable hour was refused or entry was granted but the occupier unreasonably refused to comply with a request by a person acting on behalf of OFCOM (see *Powers exercisable by warrant* at paragraph 5). The condition in paragraph (b) is that OFCOM's compliance with the conditions relating to giving notice in paragraph (a) would defeat the object of entry to the premises (e.g. where there is a risk of evidence destruction) and the condition in paragraph (c) is that OFCOM requires urgent access to the premises.

492. Sub-paragraph (3) defines the term "enforceable requirement" with reference to the duty or requirements in clause 82 and requirements imposed by a use of technology notice under clauses 64, 65 or 67.

Evidence of authority

493. Paragraph (4)(1) states that before exercising a power of entry under a warrant, an authorised person must, if requested to do so, produce evidence of their identity and outline the purpose for using this power of entry. The authorised person must also produce, and supply the occupier of the premises with, a copy of the warrant.

494. Paragraph (4)(2) states that if the occupier of the premises is not present, and neither is any other person who appears to the authorised person to be in charge of the premises, then the authorised person must leave a copy of the warrant in a prominent place on the premises.

Powers exercisable by warrant

495. Paragraph (5) lists what a warrant must allow an authorised person to do. The list is self-explanatory and includes the authorisation to enter the premises specified in the warrant and to inspect any documents which may be relevant to OFCOM's investigation.

Powers of seizure: supplementary

496. Paragraph (6) deals with powers of seizure (i.e. when a person executing a warrant seizes a document, record or other thing). Sub-paragraph (2) specifies that where the person executing a warrant seizes a document or record, they must, on request, give a receipt for it and give a copy of it to the occupier of the premises (on request).

497. Sub-paragraph (3) specifies that the person executing a warrant does not need to give an occupier of the premises a copy of the document or record if they consider that this would result in undue delay. Sub-paragraph (4) further specifies that anything seized may be retained for so long as is necessary.

Further provision about executing warrants

498. Paragraphs (7) to (13) set out further provisions relating to the execution of a warrant. Paragraph (7) requires that OFCOM's entry and search under a warrant

must be at a reasonable hour, unless entry at a reasonable hour would frustrate or seriously prejudice the purpose of the search.

499. Paragraph (8) provides that entry and search under a warrant must be within one month of its issue. Paragraph (9) allows an authorised person to take such persons, equipment and materials onto the premises as they deem to be necessary.

500. Paragraph (10) states that any person accompanying an authorised person under paragraph 9 may exercise any of the powers conferred on the authorised person by paragraph (5) provided that they are being supervised by an authorised person. Paragraph (11) states that an authorised person may use reasonable force if necessary (in connection with the exercise of a power under a warrant).

501. Paragraph (12) provides that a warrant authorises entry on only one occasion. Paragraph (13) states that if the relevant premises are unoccupied or the occupier is temporarily absent, the authorised person must leave the premises as effectively secured against trespassers as they found them.

Return of warrants

502. Paragraph (14)(1) states that after a warrant has been executed, it must be returned to the appropriate person (namely, the justice or clerk of the court who issued the warrant: see sub-paragraph (3)), and that the person who executed the warrant must write on it a statement of the powers exercised under that warrant.

503. Paragraph (14)(2) states that if the warrant has not been executed, it must be returned to the appropriate person within the time authorised for the execution of that warrant.

504. Paragraph (14)(4) states that the appropriate person must retain a search warrant returned in the circumstances stated above in sub-paragraphs (1) or (2) for 12 months from the date of its return.

505. Paragraph (14)(5) states that during that 12 month period, if the occupier of the premises stated in the warrant asks to inspect that warrant, they must be allowed to do so.

Restrictions on powers under paragraphs 2 and 3

506. Paragraph (15) applies limitations to the powers set out in paragraph (2), relating to entry and inspection of premises without a warrant, and to powers exercisable under a warrant.

507. Sub-paragraph (2) states that these powers are not exercisable in respect of a dwelling.

508. Sub-paragraph (3) excludes documents subject to legal privilege from the scope of these powers (or, in Scotland, to confidentiality of communications).

Interpretation

509. Paragraphs (16) to (18) define “premises”, “warrant” and “justice” for the purposes of this Schedule. These definitions are self explanatory. Paragraphs (19) and (20) specify some points around interpretation when paragraph (3)(1) is applied in Scotland or Northern Ireland. For Scotland, references to sworn information in writing has effect as a reference to evidence on oath and for Northern Ireland, this reference has effect as a reference to a complaint on oath.

Disclosure of information

Clause 78: Provision of information to the Secretary of State

510. The clause makes amendments to Section 24B of the Communications Act 2003 (CA 2003), which allows OFCOM to provide information to the Secretary of State that OFCOM considers may assist the Secretary of State in the formulation of policy.

511. Subsection (2) amends section 24B(2) CA 2003 so that, where information relating to a particular business has been obtained using a power under the Online Safety Bill, OFCOM may not provide this information to the Secretary of State without the consent of the person carrying on that business whilst the business is carried on. This does not affect the fact that consent must still also be obtained where the information that OFCOM intends to share has been acquired using powers in the CA 2003, the Broadcasting Act 1990, the Broadcasting Act 1996, the Wireless Telegraphy Act 2006 or Part 3 of the Postal Services Act 2011 (which were already listed in section 24B(2) of CA 2003).

512. Subsection (3) inserts a new subsection (3) into section 24B of the CA 2003. This new subsection provides that section 24B(2) does not apply, and therefore the consent of the person carrying on the relevant business is not required, where the information which OFCOM intends to share is reasonably required by the Secretary of State and:

a. was obtained by OFCOM using a power under clause 70 in order to determine a proposed threshold figure, which if met or exceeded by providers renders them liable to pay fees to OFCOM; or

b. was obtained by OFCOM using the power under clause 112(5) to require information from a provider of a regulated service in response to potential threats to national security, or to the health or safety of the public.

Clause 79: Disclosure of information

513. This clause amends section 393 of the Communications Act 2003 (CA 2003) (general restrictions on disclosure of information) to include new provisions under this Bill. Section 393 provides that, subject to specific exceptions, information obtained by OFCOM in the exercise of its functions under the CA 2003, Broadcasting Act 1990 and Broadcasting Act 1996 cannot be disclosed without the consent of the business in question.

514. Subsection (2) inserts a reference to “the Online Safety Act 2021” into section 393(1) of the CA 2003. This would mean that, subject to the exceptions detailed

below, where OFCOM has obtained information about a business by exercising its powers under this Bill, it cannot disclose this information without the consent of the business in question.

515. Subsection (3) amends the list of exceptions in section 393 of the CA 2003 so OFCOM could disclose information about a business, without its consent, for the purposes of any civil proceedings brought under this Bill.

516. Subsection (4) amends section 393 of the CA 2003 subsection (6) so as to not limit what can be published by OFCOM under Schedule 4 to the Bill. This Schedule deals with regulations specifying threshold conditions for categories of regulated services.

517. Similarly, subsection (5) amends section 393 of the CA 2003 subsection (6)(b), which ensures that section 393 of the CA 2003 does not limit the matters that may be included in, or made public as part of, a report made by OFCOM under this Bill.

Chapter 6: Enforcement Powers

Provisional notices and confirmation decisions

Clause 80: Provisional notice of enforcement action

518. Subsection (1) states that OFCOM may give a person notice that OFCOM intends to take enforcement action, through issuing a provisional notice of enforcement action to that person.

519. Subsection (2) states that (subject to the limitation in respect of prevalent and persistent terrorism or child sexual exploitation and abuse (CSEA) content set out in clause 81) OFCOM may issue a provisional notice of enforcement action to a provider of a regulated service if OFCOM considers there are reasonable grounds for believing that a provider of a regulated service has failed, or is failing to comply, with any of the 'enforceable requirements' listed in clause 82.

520. In addition, subsections (3) and (4) provide that OFCOM may issue a provisional notice of enforcement action to a person if OFCOM reasonably consider that the person is failing to comply with their duties under an information notice issued to them under clause 70, or OFCOM reasonably consider that the person has not rendered the assistance which it is required to give to a skilled person under clause 74.

521. Subsection (5) specifies that the provisional notice of enforcement action must specify the duty or requirement that OFCOM considers the person has breached, OFCOM's reasons for holding that opinion, and the steps OFCOM considers the person needs to take to comply with the relevant duty or requirement, or to remedy the breach.

522. Subsection (6) provides that the provisional notice of enforcement action may further state that OFCOM proposes to impose a penalty on the person and, if it does,

the notice must state OFCOM's reasons for proposing a penalty and the amount of penalty OFCOM propose, detailing any aggravating or mitigating factors they propose to consider in determining the final amount of the penalty.

523. Subsection (7) states that a provisional notice of enforcement action must state that the person who receives the notice may make written representations on the matters contained within the notice and the notice must specify the period within which such representations may be made.

524. Subsection (8) provides that a provisional notice of enforcement action may be given in respect of a breach of multiple enforceable requirements set out in clause 82.

525. Subsection (9) provides that, in the case of a continuing breach of a relevant duty or enforceable requirement, a provisional notice of enforcement action may be issued in respect of any period of time during which the breach was occurring. The notice must specify the period of time which it is concerned with.

526. Subsection (10) states that where a provisional notice of enforcement action is issued to a person (the first notice), OFCOM may only issue a further provisional notice of enforcement action in respect of a breach of the same duty or requirement if: it relates to a separate breach occurring after the first notice was issued; the first notice dealt with a continuous breach and the further notice arises out of a continuation of the breach after the end of the period of breach specified in the first notice; or the first notice has been withdrawn without OFCOM imposing a penalty via the issuing of a confirmation decision.

Clause 81: Prevalent and persistent terrorism or child sexual exploitation and abuse content

527. Subsection (1) explains that this clause applies where OFCOM reasonably considers that a provider of a regulated user-to-user or search service is failing to comply with its safety duties relating to illegal content (as set out in clause 9) in relation to terrorism or CSEA content, based on evidence demonstrating the prevalence and persistence of terrorism and/or CSEA content on the service or in the search results of the service.

528. Subsection (2) states that OFCOM may not give a provider of a regulated user-to-user service a provisional notice of enforcement action under clause 80 if the provider is complying with all the other enforceable requirements listed in clause 82. Subsection (4) makes it clear, however, that in such circumstances, it would be open to OFCOM to take action in respect of the provider's breaches of its safety duties relating to illegal content (under clause 9) in relation to terrorism or CSEA content by issuing the provider with a technology warning notice under clause 63.

529. Nonetheless, should OFCOM be of the opinion that there are reasonable grounds for believing that a provider who is failing to comply with its illegal content safety duties with respect to terrorism or CSEA content is also in breach of one of the other enforceable requirements listed in clause 82, OFCOM may issue a provisional notice of enforcement action in relation to this breach of another enforceable requirement. Subsection (5) makes it clear that, in these circumstances, OFCOM is

able to impose both a technology warning notice under clause 63 and a provisional notice of enforcement action.

Clause 82: Requirements enforceable by OFCOM against providers of regulated services

530. Under clause 80, OFCOM may give a provisional notice of enforcement action to a provider of a regulated service if OFCOM believes that the provider has failed, or is failing to comply with, any "enforceable requirement". OFCOM may then impose a confirmation decision under clause 83 in respect of the failure to comply with an enforceable requirement. This clause sets out the "enforceable requirements" referred to in clauses 80 and 83. By way of example, these include, among other things, the duties to carry out and report on risk assessments, the safety duties and duties about rights to freedom of expression and privacy.

Clause 83: Confirmation decisions

531. As set out in clause 80, OFCOM may give a provisional notice of enforcement action to a provider of a regulated service if it believes that that the provider has failed, or is failing to comply with any "enforceable requirement" or is breaching a relevant duty relating to information notices or skilled persons' reports. This provisional notice of enforcement action is referred to as a "notified requirement". This clause sets out how OFCOM can subsequently issue a confirmation decision.

532. A confirmation decision is a formal notification that the relevant person has failed or is still failing to comply with a notified requirement (set out in the provisional notice of enforcement) and the period allowed for representations has expired: see subsection (1). A confirmation decision can include a notice imposing requirements for the provider to take steps to comply with a notified requirement and/or to pay a penalty: see subsection (3) and (4).

533. Subsection (5) details the circumstances in which a confirmation decision may require a person to either take steps to comply with a notified requirement or to remedy the failure.

534. Subsection (6) states the circumstances in which a confirmation decision may require the person to pay a penalty, of an amount specified by OFCOM.

535. Subsection (7) sets out that, where a confirmation decision includes requirements to comply or remedy the failure, then it must:

a. give OFCOM's reasoning for the requirements it is imposing and specify the notified requirement;

b. require the person to comply with the notified requirement, or remedy the failure, specifying the time period for that action; and

c. detail the rights of appeal, and set out the consequences of non-compliance. This could include further information about the further kinds of enforcement action that OFCOM could take.

536. Subsection (8) sets out that where a confirmation decision includes a requirement to pay a penalty, then it must:

a. give OFCOM's reasoning for its decision and specify the notified requirement;

b. state the reasons for the amount of the penalty, and how and when it should be paid; and

c. detail the rights of appeal, and set out the consequences of not paying the penalty. This could include further information about the further kinds of enforcement action that OFCOM could take.

537. Subsection (10) states that a confirmation decision may only impose requirements in relation to regulated services in the UK or regulated services that affect users in the UK.

538. Subsection (11) states that a confirmation decision may not impose a requirement to use technology to monitor content with a view to taking down such content or removing such content from search results (as appropriate).

539. Subsection (12) provides that a confirmation decision may impose separate penalties for failure to comply with separate notified requirements but where a provisional notice of enforcement action is given in respect of a period of continuing failure, then only one penalty may be imposed in respect of that period: see subsection (13). However, subsection (14) states that OFCOM can impose a daily penalty where a confirmation decision imposes requirements in respect of ongoing failures. This can be imposed after a period specified in the confirmation decision (which will allow the relevant service provider the opportunity to come into compliance first).

Clause 84: Compliance with certain requirements of confirmation decisions

540. This clause sets out how a person should comply with the requirements specified in a confirmation decision.

541. Subsection (1) states that the recipient of a confirmation decision has a duty to comply with a requirement set out in the confirmation decision to take steps to remedy a breach which has been the subject of a provisional notice of enforcement action. OFCOM may enforce compliance with this duty in civil proceedings by virtue of subsection (2).

542. Subsection (3) states that OFCOM may issue a person with penalty notice if it is satisfied that the person has not complied with a requirement in a confirmation decision to take steps to remedy a breach which has been the subject of a provisional notice of enforcement action. Subsection (4) notes that, for the purposes of this clause, a penalty notice is a notice which requires the recipient to pay OFCOM a penalty of an amount in sterling which is specified in the notice.

543. Subsection (5) states that a penalty notice must:

a. give OFCOM's reasoning for their decision to issue a penalty notice and state the reasons for the amount of the penalty;

b. specify how and when the penalty should be paid (noting that, by virtue of subsection (6) the period within which the penalty must be paid cannot be less than 28 days); and

c. detail the rights of appeal, and set out the consequences of not paying the penalty. This could include information about the further kinds of enforcement action that OFCOM could take.

Clause 85: Amount of penalties

544. As set out in clauses 83 and 84 the regulator will be able to impose penalties in a confirmation decision or a penalty notice: see subsection (1). This clause sets out the amount of a penalty that can be imposed on a person in such notices.

545. Subsection (2) sets out the things that OFCOM will need to take into account when determining the size of the penalty. This includes any representations made by the person or evidence provided by the person, any steps taken by the person to comply with the requirements set out in the provisional notice of enforcement action or confirmation decision, any steps taken to remedy the failure and the effects of the failure in respect of which the penalty is being imposed. Subsection (3) states that OFCOM must impose a penalty that it considers to be appropriate and proportionate to the failure (or failures) in respect of which the penalty is imposed.

546. Subsection (4) states that the maximum penalty that OFCOM can impose on the provider of a regulated service is the greater of £18 million and 10% of the person's qualifying worldwide revenue. Subsection (5) means that if the person does not have a clear accounting period the maximum penalty OFCOM can impose is £18 million. Subsection (6) states that the maximum penalty OFCOM can impose on other persons (not regulated service providers) is £18 million. These provisions also apply to determine the total maximum amount of daily penalties that may be imposed by OFCOM in a confirmation decision: see subsection (11).

547. Subsection (7) includes further detail on how "qualifying worldwide revenue" will be calculated for the purposes of subsection 4(b) of this clause. For example, if the duration of the most recent complete accounting year is less than a year, then the amount should be proportionately increased: see subsection (8). Further, if the duration of the most recent accounting year is longer than a year, then the amount should be proportionately decreased. The term "qualifying worldwide revenue" will be defined in regulations made by the Secretary of State (see subsection (14)) following consultation with OFCOM (see subsection 15).

548. Subsection (9) provides that where the qualifying worldwide revenue for an accounting period cannot be agreed between the individual and OFCOM, then OFCOM will determine the amount.

549. Subsection (10) confirms that a penalty imposed by a confirmation decision clause 83 may not exceed the amount of the penalty that was initially proposed in the

provisional notice of enforcement action given to the provider of the regulated service clause 80.

550. Subsection (11) confirms that the total maximum amount of daily penalties imposed by OFCOM under clause 83(14) will be determined in the same way as the maximum amount of the penalties set out in subsections (4) to (6) of clause 85.

551. Subsection (12) refers to Section 392 of the Communications Act 2003, which requires OFCOM to produce guidelines setting out how they determine penalty amounts.

552. Subsection (13) states that "accounting period" means a period in which a person is required to prepare accounts (by law or by the constitution of the entity) either in respect of the entity or in respect of the individual's business of providing a regulated service (as appropriate).

Clause 86: Amount of penalties: group of entities

553. This clause applies where two entities are jointly liable for a penalty imposed by a confirmation decision or a penalty notice. This may occur where OFCOM deems a parent company jointly liable for the breach of its subsidiary (as per clause 119), or where OFCOM deems a subsidiary company to be jointly liable for the breach of its fellow subsidiary or parent company (as per clause 121). This clause sets out how penalties are to be calculated in such a scenario.

554. Subsection (3) states that the maximum amount of the penalty in such cases is the greater of £18 million and 10% of the "qualifying worldwide revenue" of the group of entities of which the two entities are members.

555. Subsection (4) defines the "qualifying worldwide revenue" for a group of entities as the amount of the group's qualifying worldwide revenue for the most recent complete accounting period of the liable entities or, if OFCOM are deciding the amount of the penalty at a time when the first accounting period has not ended yet, the amount that OFCOM estimate to be the group's likely qualifying worldwide revenue for that period.

556. Subsection (5) provides for circumstances where the accounting periods of the liable entities within a group are different. In such circumstances, OFCOM can decide which entity or entities' accounting period to use for the purposes of calculating the "qualifying worldwide revenue".

557. Subsection (7) states that "qualifying worldwide revenue" has the same meaning as in clause 85, i.e. it will be defined in regulations made by the Secretary of State following consultation with OFCOM. The regulations may include details for applying this term to a group of entities.

558. Subsection (9) confirms that for the purposes of this clause, section 1162 and Schedule 7 to the Companies Act 2006 should be read with the relevant modifications, if it is to be applied to an entity outside of the United Kingdom.

Clause 87: Penalties: further provision

559. This clause sets out how payment of penalties can be enforced.

560. Subsection (2) sets out that in England and Wales, a penalty can be recovered if the county court or High Court orders payment.

561. Subsection (3) confirms that in Scotland, a penalty can be enforced in the same way as an extract registered decree arbitrarily bearing a warrant for execution, that would be issued by the sheriff court.

562. Subsection (4) sets out that in Northern Ireland, a penalty can be recovered if the county court or High Court orders payment.

Non-payment of fee

Clause 88: Notice about non-payment of fee

563. Clause 52 explains where OFCOM may require a provider of a regulated service to pay a fee. This clause sets out OFCOM's power to issue a notice where a provider of a regulated service does not pay its fee to OFCOM.

564. Subsection (1) confirms that OFCOM can give a notice to a provider of a regulated service where they are liable to pay a fee and OFCOM believes that they have not paid the full amount.

565. Subsection (2) states that OFCOM must specify the outstanding amount and specify a period within which it should be paid. Subsection (3) provides that the notice must invite written representations from the provider within a specified timeframe. One notice may be given in respect of more than one liability to pay a fee: see subsection (4).

Clause 89: Penalty notice for non-payment of fee

566. This clause sets out the circumstances under which OFCOM can give a provider a penalty notice for not paying a fee.

567. Subsection (1) states that a penalty notice can be given under this section, if following a notice specifying the outstanding amount of fee to be paid (as per clause 88), the period for the provider giving representations has expired and OFCOM is satisfied that the fee has still not been paid to them.

568. Subsection (3) sets out what OFCOM must take into account when determining the penalty fee and subsection (4) provides for further detail on what the penalty notice should include such as the amount of the fee, the reasons for giving a penalty notice and the time period for paying it.

569. Subsection (7) makes clear that the definitions set out at clause 85(3) to (9) and the provisions at clause 86 and clause 87 also apply in relation to this clause.

570. Subsection (8) makes clear that this clause does not impact OFCOM's power to bring proceedings for the recovery of the amount due to OFCOM. However, as set out in subsection (9), they must not bring such proceedings until the provider has been notified of how much is due to be paid (clause 88).

Non-compliance with use of technology notice

Clause 90: Penalty notice for failure to comply with use of technology notice

571. Subsections (1) and (2) states OFCOM may give a service provider a penalty notice requiring it to pay a penalty, if OFCOM has given a service provider a use of technology notice under clause 64, 65 or 67 relating to a regulated service and OFCOM is satisfied that, at any time during which the notice is in force, the provider is failing to comply with the notice.

572. Subsection (3) sets out that before OFCOM can issue the penalty notice, OFCOM must notify the provider that they intend to give a penalty notice under this section, specifying the grounds for doing so and indicating the amount of the proposed penalty. OFCOM must give the provider an opportunity to make representations, consider any representations made together with any steps taken by the provider towards complying with the use of technology notice.

573. Subsection (4) notes that nothing in this section prevents OFCOM from also giving the provider a further use of technology notice under clause 67 in addition to issuing a penalty notice.

574. Subsection (5) sets out the information that the penalty notice must contain, including (a) OFCOM's reasons for its decision to give the penalty notice; (b) the reasons for the amount of the penalty; (c) specifying the period within which the penalty must be paid and (d) the rights of appeal of such a notice.

575. Subsection (6) sets out that the period specified under subsection (5)(c) must be not less than 28 days beginning with the day on which the penalty notice is given. Subsection (7) states that the final penalty imposed must not be greater than the amount proposed in the notice under subsection (3).

576. Subsection (8) states that a penalty issued to a provider of a regulated service under this clause must be appropriate and proportionate (clause 85 (3)) and no more than either £18 million or 10% of the provider's or relevant group of entities' qualifying worldwide revenue, whichever is greater.

Business disruption measures

Clause 91: Service restriction orders

577. This clause sets out the circumstances in which OFCOM may apply to the court for a "service restriction order". These are orders that require providers of "ancillary services" (persons providing, for example, payment or advertising services) to implement measures aimed at disrupting the business of a non-compliant provider's operations in the UK.

578. This clause sets out the circumstances in which OFCOM may apply to the court for a "service restriction order". These are orders that require providers of "ancillary services" (persons providing, for example, payment or advertising services) to implement measures aimed at disrupting the business of a non-compliant provider's operations in the UK.

579. Subsection (1) confers a power on OFCOM to apply to the court for a service restriction order where it considers that the grounds in subsection (3) or (4) apply in relation to a regulated service (as explained below).

580. Subsection (2) provides a definition of a "service restriction order". This is defined as an order imposing requirements on persons who provide an ancillary service to a regulated service.

581. Subsection (3) specifies the first set of grounds on which OFCOM may seek a service restriction order. These grounds are that OFCOM considers that a provider of a regulated service has failed to comply with an enforceable requirement (these are set out in clause 82 and include, for example, safety duties about illegal content and safety duties protecting children), this failure is continuing, and the provider has either:

a. failed to comply with a requirement imposed by a confirmation decision (see clause 83), or

b. failed to pay a penalty imposed by a confirmation decision (see clause 83) relating to the failure (and the confirmation decision did not impose any requirements on the provider), or

c. the provider would be likely to fail to comply with a confirmation decision if given, or the risk of harm to individuals in the UK means it is appropriate to apply for a service restriction order without having given a provisional notice of enforcement or a confirmation decision. For example, for expediency where the risk of harm is so severe.

582. Subsection (4) specifies the second set of grounds on which OFCOM may seek a service restriction order. These grounds are that OFCOM considers that a provider of a regulated service has failed to comply with a use of technology notice (under clause 64, 65 or 67), and the failure is continuing.

583. Subsection (5) sets out what information an application by OFCOM to the court for a service restriction order must include. The requirements are that an application must:

a. Specify the regulated service in relation to which the application is made, specify the provider of that regulated service and contain evidence that the grounds in subsection (3) or (4) are met, and

b. Specify the persons on whom OFCOM considers the requirements of the order should be imposed, contain evidence for why OFCOM considers these persons provide an ancillary service, specify what this ancillary service is and detail the requirements that OFCOM considers should be imposed on these

persons. Where OFCOM has not given notice to the non-compliant provider or relevant ancillary services, it must state why no notice has been given.

584. Subsection (6) specifies what the court must be satisfied of before it may make a service restriction order imposing requirements on a person. The court must be satisfied that the grounds in subsection (3) or (4) are met; that is, that the person in question provides an ancillary service and that the making of such an order is appropriate for preventing harm to individuals in the UK. Where OFCOM is seeking to argue that a provider would be likely to fail to comply with a confirmation decision if one were given, or the circumstances of the failure mean it is appropriate to apply for a service restriction order without giving a confirmation decision, the court must also be satisfied that it is appropriate to make a service restriction order before a provisional notice of enforcement or a confirmation decision. Where no notice of the application has been given to the non-compliant provider or the person(s) on whom requirements are being imposed (e.g. where OFCOM cannot contact them), the court must also be satisfied that it is appropriate to make an order without notice).

585. Subsection (7) sets out further matters that the court must take into account when considering whether to make a service restriction order and when considering what provision the order should contain. The court must take into account the rights and obligations of all relevant parties, including those of the non-compliant provider, UK users of the relevant service, and providers of an ancillary service on whom the court is considering imposing the requirements.

586. Subsection (8) sets out what information a service restriction order must include. This includes the identity of the non-compliant provider, the identity of the ancillary service provider on whom the requirements are imposed and the ancillary service(s) to which the requirements relate, the steps to be taken in order to withdraw the ancillary service from the non-compliant provider, the date by which the requirements must be complied with and the date on which the order expires or the time period for which the order has effect.

587. Subsection (9) states that a service restriction order may specify steps or arrangements that could require the termination of an agreement or prohibit the performance of such an agreement. This would in effect mean the ancillary service provider is not obliged to fulfil its contractual obligations under its agreement with the regulated provider. It is irrelevant whether the agreement was made before the coming into force of this section. Subsection (9)(b) states that these steps or arrangements should be limited so far as possible to the operations of the relevant service as it affects users who are in the UK.

588. Subsection (10) imposes an obligation on OFCOM to inform the Secretary of State of any service restriction order as soon as reasonably possible after the order has been made by the court.

589. Subsection (11) defines an “ancillary service” as one that facilitates the provision of a regulated service or part of it (whether directly or indirectly) or displays content relating to that service or part of it.

590. Subsection (12) provides a non-exhaustive list of ancillary services. This list includes payment service providers, search engines, user to user services which make content relating to a regulated service available to users (which could cover social media platforms) and advertising services (such as ad servers or ad networks).

591. Subsection (13) defines "the court" for the purposes of this clause. For England and Wales this is the High Court or the county court, for Northern Ireland the High Court or county court, and for Scotland the Court of Session or a sheriff.

Clause 92: Interim service restriction orders

592. This clause sets out the circumstances in which OFCOM may apply to the courts for an interim service restriction order.

593. Subsection (1) confers a power on OFCOM to apply to the court for an interim service restriction order in relation to a regulated service where it considers that the grounds in (3) or (4) apply to the service.

594. Subsection (2) defines an "interim service restriction order". This is defined as an interim order imposing requirements on one or more persons who provide an ancillary service in relation to a regulated service.

595. Subsection (3) specifies the first set of grounds on which OFCOM may seek an interim service restriction order. These grounds are that OFCOM considers it to be likely that the provider of a regulated service is failing to comply with an enforceable requirement (set out in clause 82) and the level of risk of harm to UK users resulting from this likely failure, and the nature and severity of that harm, mean that it would not be appropriate to establish the failure before applying for the order.

596. Subsection (4) sets out further grounds on which OFCOM may seek an interim service restriction order. These grounds are that it is likely that a provider of a regulated service is failing to comply with a use of technology notice (see clause 64, 65 or 67) and the level of risk of harm to individuals in the UK resulting from this likely failure, and the nature and severity of that harm, are such that it would not be appropriate to establish the failure before applying for the order.

597. Subsection (5) sets out what information must be included in an application to the court by OFCOM for an interim service restriction order. The application must:

a. Specify the regulated service in relation to which the application is made, the provider of that service and contain evidence that either grounds in subsections (3) or (4) are met, and;

b. Specify the persons on whom, in OFCOM's opinion, the requirements of the order should be imposed, contain evidence that these persons provide an ancillary service in relation to the relevant service, specify what this ancillary service is and contain details of the requirements OFCOM considers the order should impose on these persons.

c. If an application has been made without giving notice to the non-compliant provider or the ancillary service provider, set out why no notice has been given.

598. Subsection (6) sets out what the court must be satisfied of before it can proceed to issue an interim service restriction order. The court must be satisfied that the grounds in either subsection (3) or (4) are met and that the person on whom the order will be imposed provides an ancillary service, and that there are prima facie grounds why an application for a service restriction order under clause 91 would be successful. The court must also be satisfied that the risk of harm to UK individuals, and the nature and severity of that harm, mean it would not be appropriate to wait for the failure to be established before making the order and, if no notice has been given, that it is appropriate to make an interim order without notice.

599. Subsection (6) sets out what the court must be satisfied of before it can proceed to issue an interim service restriction order. The court must be satisfied that the grounds in either subsection (3) or (4) are met and that the person on whom the order will be imposed provides an ancillary service, and that there are prima facie grounds why an application for a service restriction order under clause 91 would be successful. The court must also be satisfied that the risk of harm to UK individuals, and the nature and severity of that harm, mean it would not be appropriate to wait for the failure to be established before making the order and, if no notice has been given, that it is appropriate to make an interim order without notice.

600. Subsection (7) provides that an interim service restriction order will cease to have effect on the earlier of either the date specified in the order (or the date on which the time period specified in the order expires), or the date on which the court makes a service restriction order under clause 91 that imposes requirements on the persons who are subject to the interim service restriction order (or dismisses the application for such an order).

601. Subsection (8) provides that subsections (7) to (10) of clause 91 apply to the making of interim service restriction orders. (For example, these subsections require the court to consider the rights and obligations of parties to the order, set out what information an order must contain, that the steps required by an order can include steps that could require the termination of an agreement and that the Secretary of State must be informed of the making of an order).

602. Subsection (9) provides that “ancillary service” and “the court” are defined in the same way as in clause 91.

Clause 93: Access restriction orders

603. This clause sets out the circumstances in which OFCOM may apply to the courts for an “access restriction order”. An access restriction order can require third parties who provide an “access facility” to take steps to impede access to a non-compliant regulated service. Access restriction orders seek to impede the operation of a regulated service by preventing, restricting or deterring individuals in the UK from accessing that service.

604. Subsection (1) confers a power on OFCOM to apply to the court for an access restriction order where it considers that the grounds in clause 91(3) or clause 91(4) apply. These are where the provider:

a. has failed to comply with a requirement imposed by a confirmation decision (see clause 83), or failed to pay a penalty imposed by a confirmation decision (see clause 83) relating to the failure (and the confirmation decision did not impose any requirements on the provider); or

b. would be likely to fail to comply with a confirmation decision if given, or the risk of harm to individuals in the UK means it is appropriate to apply for a service restriction order without having given a provisional notice of enforcement action or confirmation decision (for example, for expediency where the risk of harm is so severe); or

c. has failed to comply with a use of technology notice (under clause 64, 65 or 67), and the failure is continuing.

d. OFCOM must also consider that either (i) a service restriction order issued under clause 91 or an interim service restriction order issued under clause 92 is not sufficient to prevent significant harm to individuals in the UK, or (ii) the likely consequences of such a failure are such that they would be unlikely to be sufficient to prevent significant harm to individuals in the UK.

605. Subsection (2) defines an “access restriction order”. This is defined as an order imposing requirements on one or more persons who provide an “access facility” in relation to a regulated service. Subsection (10) defines an “access facility” for the purposes of this clause. This is defined as a facility that can be withdrawn, adapted or manipulated by the provider of the facility in a way that impedes access by UK users to the relevant service. Subsection (11) provides a non-exhaustive list of access facilities, including internet access services and app stores.

606. Subsection (3) specifies what information an application to the court for an access restriction order by OFCOM must include. The application must:

a. Specify the regulated service about which the application is made, the provider of that service and specify the grounds on which the application is made and contain evidence of those grounds.

b. Specify the persons on whom the requirements of the order should be imposed, contain evidence for why OFCOM considers these persons provide an access facility and specify what this access facility is, and contain details of the requirements OFCOM thinks should be imposed on these persons.

c. If an application has been made without giving notice to the non-compliant provider or the person(s) providing an access facility, set out why no notice has been given.

607. Subsection (4) specifies what the court must be satisfied of before it may make an access restriction order imposing requirements on a person. The court must be satisfied that the grounds in subsection (1) are met, that the person provides an

access facility and that the making of this order is appropriate for preventing harm to individuals in the UK. If an access restriction will be imposed before a provisional notice of enforcement action or confirmation decision is given, the court must also be satisfied that this is appropriate and, if no notice has been given, that it is appropriate to make an interim order without notice.

608. Subsection (5) specifies that the court must take into account the rights and obligations of all relevant parties when considering whether to make an access restriction order and what provision it should contain. This includes the rights and obligations of the non-compliant provider, the persons providing an access facility and UK users of the relevant service.

609. Subsection (6) specifies what information an access restriction order must contain. This information includes the identity of the non-compliant provider, the identity of the persons providing an access facility on whom the requirements are imposed, and the steps to be taken, or arrangements to be put in place, in order to impede user access to the relevant service. The order must also specify the date by which the order must be complied with and the date on which it expires (or the time period over which the order has effect).

610. Subsection (7) provides that an access restriction order may include steps or arrangements that require the termination of an agreement or prohibit the performance of such an agreement. It is irrelevant whether the agreement was made before the coming into force of this section. Subsection (7)(b) states that these steps or arrangements are to be limited, so far as possible, to only impede the access of UK users of the relevant service and subsection (7)(c) states that they should not affect UK users' ability to access other internet services, so far as this is possible.

611. Subsection (8) imposes an obligation on OFCOM to inform the Secretary of State of any access restriction order as soon as reasonably possible after the order has been made.

612. Subsection (9) provides that OFCOM may require providers of access facilities to notify their users who attempt to access the relevant service that an access restriction order is in place (and refer to the relevant confirmation decision, if the order was made on the basis that the provider has failed to comply with a requirement imposed by a confirmation decision under clause 83).

613. Subsection (12) defines "the court", "facility" and "internet access service" for the purposes of this clause. "The court" is defined as, for England and Wales the High Court or the county court, for Northern Ireland the High Court or county court, and for Scotland the Court of Session or a sheriff. "Facility" is defined as any service, infrastructure or apparatus that enables users to access a regulated service. "Internet access service" is defined as a service that provides access to virtually all of the end points of the internet (e.g. ISPs).

Clause 94: Interim access restriction orders

614. This clause sets out the circumstances in which OFCOM may apply to the courts for an interim access restriction order.

615. Subsection (1) confers a power on OFCOM to apply to the court for an interim access restriction order where it considers that the grounds in (a) and (b) are met. First, (a) requires the grounds in subsection clause 92(3) or (4) to apply. These are the same as listed above under clause 91, namely where the provider:

a. has failed to comply with a requirement imposed by a confirmation decision (see clause 82), or failed to pay a penalty imposed by a confirmation decision (see clause 82) relating to the failure (and the confirmation decision did not impose any requirements on the provider), or

b. would be likely to fail to comply with a confirmation decision if given, or the risk of harm to individuals in the UK means it is appropriate to apply for a service restriction order without having given a provisional notice of enforcement action or a confirmation decision (for example, for expediency where the risk of harm is so severe), or

c. has failed to comply with a use of technology notice (under clause 64, 65 or 67), and the failure is continuing.

616. Second, (b) requires OFCOM to also be satisfied that either:

a. an interim service restriction order or service restriction order was imposed and was not sufficient to prevent significant harm to UK users arising from the breach, or

b. in all circumstances, imposing an interim service restriction order or service restriction order would be unlikely to prevent significant harm to UK users arising from the breach.

617. Subsection (2) defines an “interim service restriction order” as an interim order imposing requirements on persons who provide an access facility in relation to a regulated service.

618. Subsection (3) specifies that an application to the court for an interim access restriction order by OFCOM must:

a. Specify the regulated service, the provider of that service and specify the grounds on which the application is based and contain evidence of such grounds; and

b. Specify the persons on whom the requirements of the order should be imposed, contain evidence that these persons provide an access facility, specify what this access facility is and contain details of the requirements that OFCOM considers should be imposed on these persons. If no notice has been given to the non-compliant provider or the provider of an access facility, state why no notice was given.

619. Subsection (4) specifies what the court must be satisfied of before it may make an interim access restriction order imposing requirements on a person. The court must be satisfied that the grounds in subsection 92(3)(a) or (4)(a) are met, as to the ground in subsection (1)(b)(i) or (ii) (as the case may be), that the person in

question provides an access facility, that there are prima facie grounds why an application for an access restriction order under clause 93 would be successful, and that the level of risk of harm to individuals in the UK makes it appropriate not to wait for the failure to be established before making the order. If no notice of the application has been given, the court must also be satisfied that it is appropriate to make an interim order without notice.

620. Subsection (5) specifies that an interim access restriction order will cease to have effect on whichever is earlier of: (i) the date specified in the order, or (ii) the date on which the court makes an access restriction order under clause 93 that imposes requirements on the same persons (or dismisses the application for such an order).

621. Subsection (6) provides that subsection (5) to (8) of clause 93 apply to the making of an access restriction order. For example, these subsections require the court to consider the rights and obligations of parties to the order, set out what information an order must contain, that the steps required by an order can include steps that could require the termination of an agreement, and that the Secretary of State must be informed of the making of an order.

622. Subsection (7) provides that OFCOM may require providers of access facilities to notify their UK users who attempt to access the relevant service that an access restriction order is in place.

623. Subsection (8) provides that for the purposes of this clause, "access facility" and "the court" have the same meaning as in clause 93.

Clause 95: Interaction with other action by OFCOM

624. This clause explains how business disruption orders interact with OFCOM's other enforcement powers.

625. Subsection (1) explains that, where OFCOM exercises its powers to apply to the courts for business disruption orders under clauses 91 to 94 in respect of a providers' failure to comply with an enforceable requirement (clause 82), it is not precluded from also issuing the relevant regulated provider with either a confirmation decision under clause 83 or a penalty notice under clause 84.

626. Subsection (2) explains that, where OFCOM exercises its powers to apply for business disruption orders under clauses 91 to 94 in respect of a providers' failure to comply with a Use of Technology Notice under clauses 64, 65 or 67, it is not precluded from also issuing a Further Use of Technology Notice under clause 67.

Publication of enforcement action

Clause 96: Publication of details of enforcement action

627. Where OFCOM has taken enforcement action, it may publish the details of this enforcement action. This is to provide transparency to industry on OFCOM's

enforcement activities. This clause sets out where this will apply and how OFCOM must act.

628. Subsection (1) states that this applies where a confirmation decision, penalty notice, service restriction notice, or an access restriction notice have been issued.

629. Subsections (2) and (3) state that OFCOM must publish details identifying the person and the failure that the enforcement action relates to, and the action that has been taken. However, commercially sensitive data, or content that OFCOM believes is not appropriate for publication, should not be published.

630. Where OFCOM has given a person a provisional notice of enforcement action under clause 80 but taking no enforcement action against the person, OFCOM may publish details identifying the person and describing the reasons for the provisional notice: see subsection (4).

Guidance

Clause 97: Guidance about enforcement action

631. OFCOM must publish guidance about how it will use its enforcement powers.

632. Subsection (2) confirms that the guidance should give information about the factors OFCOM will take into account when taking or considering enforcement action. This enforcement action will relate to the failure to comply with the "enforceable requirements" set out in clause 82. Subsection (3) adds that the guidance must include how OFCOM will take into account the possible or actual impact of such a failure to comply with a relevant duty on children.

633. Before producing the guidance, OFCOM must consult with the Secretary of State and any persons OFCOM considers appropriate: see subsection (4). OFCOM may revise and replace the guidance and must also publish the guidance: see subsection (5).

634. Subsection (6) confirms that guidance prepared by OFCOM under Section 392 of the Communications Act 2003, relating to penalties imposed, can be included within the guidance required by this clause.

635. Subsection (7) states that when exercising, or deciding to exercise their enforcement functions, OFCOM must have regard to the guidance it has produced.

Chapter 7: Committees, research and reports

Clause 98: Advisory committee on disinformation and misinformation

636. This clause places an obligation on OFCOM to form an advisory committee on disinformation and misinformation. The government is placing this obligation on OFCOM because the spread of inaccurate information, regardless of intent, is particularly concerning. The clause sets out what OFCOM should consider when

appointing committee members, what the functions of the committee are, and what the committee's reporting obligations are.

637. Subsection (1) places a duty on OFCOM to establish and maintain an advisory committee on disinformation and misinformation.

638. Subsection (2) instructs OFCOM to appoint a committee chair. The number of members apart from the chair is at OFCOM's discretion.

639. Subsection (3) instructs OFCOM to consider three types of members when making appointments to the advisory committee: people representing providers of regulated services, people representing the interests of users of regulated services, and experts on the prevention and handling of disinformation and misinformation online.

640. Subsection (4) outlines the function of the advisory committee, which is to provide advice to OFCOM about how providers of regulated user-to-user services should deal with disinformation and misinformation present on their services, how providers of regulated search services should deal with disinformation and misinformation that may be encountered in or via search results, how OFCOM should use its transparency reporting powers in relation to disinformation and misinformation, and how OFCOM should use its media literacy functions to counter such disinformation and misinformation.

641. Subsection (5) places a duty on the advisory committee to publish a report within 18 months of it being established, and to report periodically after that.

Clause 99: Research about users' experiences of regulated services

642. This clause will amend Section 14 of the Communications Act 2003 (consumer research) to require OFCOM to arrange for research into United Kingdom users' opinions and experiences relating to regulated services.

643. Subsection (2) ensures that OFCOM must make arrangements to understand:

a. public opinion about regulated services;

b. United Kingdom users' experiences of using regulated services;

c. United Kingdom users' experiences of how providers of regulated services have handled their complaints; and

d. other interests and experiences of United Kingdom users of regulated services which are connected with their experiences of using such services.

644. Subsection (2) also ensures that OFCOM must include, in its annual report to Parliament, under paragraph 12 of the Schedule to the Office of Communications Act 2002, a statement of such research carried out.

645. Subsection (3) signposts to the definitions of "regulated service", "provider", and "United Kingdom user".

Clause 100: OFCOM's transparency reports

646. This clause places a duty on OFCOM to produce transparency reports and details what those reports should contain.

647. Subsection (1) places a duty on OFCOM to produce transparency reports based on information contained in the transparency reports which have been produced by providers of regulated services in accordance with clause 49.

648. Subsection (2) says that OFCOM's transparency report must contain a summary of conclusions drawn from the transparency reports it has asked regulated providers to publish, identifying any patterns or trends. It must also highlight good industry practice. OFCOM may also include any other information from providers' transparency reports which it deems appropriate.

649. Subsection (3) says OFCOM must publish its first transparency report within a year of the publication of the first transparency report by a provider under clause 49, and OFCOM must publish a report at least once a year after that.

650. Subsection (4) places a duty on OFCOM to publish its annual transparency report, and leaves the manner of publication to OFCOM's discretion.

651. Subsection (5) signposts that further provisions about reports can be found in clause 102.

Clause 101: OFCOM's report about researchers' access to information

652. This clause relates to OFCOM's research on and reporting of the level of access independent researchers have into matters relating to the online safety of regulated services.

653. Subsection (1) places a duty on OFCOM to prepare a report on the manner and extent to which independent researchers are currently able to obtain information from providers of regulated services to inform their research into online safety matters; the legal and other issues which currently constrain the sharing of information for such purposes; and the extent to which greater access to information for such purposes might be achieved.

654. Subsection (2) defines the term "independent research".

655. Subsection (3) lists the people OFCOM must consult during the preparation of the report, including the Information Commissioner; the Centre for Data Ethics and Innovation; United Kingdom Research and Innovation; people who appear to OFCOM to have relevant expertise; people representing providers of regulated services; and anyone else that OFCOM considers appropriate.

656. Subsection (4) places an obligation on OFCOM to publish the report within two years of this clause coming into force.

657. Subsection (5) states that OFCOM must publish the report in whatever way they consider appropriate.

658. Subsection (6) states that OFCOM must send a copy of the report to the Secretary of State; and the Secretary of State must lay it before Parliament.

659. Subsection (7) signposts further provision about this report in clause 102.

660. Subsection (8) states that, following the publication of the report, OFCOM may prepare guidance about the issues dealt with by the report for providers of regulated services and people carrying out independent research into online safety matters.

661. Subsection (9) states that if OFCOM decides to prepare such guidance, it must consult people in the same manner as described in subsection (3); publish that guidance (and any revised guidance); and include in each transparency report under clause 100 an assessment of the effectiveness of the guidance.

662. Subsection (10) states that subsection (9)(a) also applies if OFCOM decides to revise guidance under this clause.

Clause 102: Reports by OFCOM

663. This clause relates to reports that OFCOM publishes about online safety matters.

664. Subsection (2) provides that when publishing reports mentioned in subsection (5), OFCOM must consider excluding matters which are confidential under subsections (3) and (4).

665. Subsections (3) and (4) provide that a matter is confidential if it relates to the affairs of a particular body or private affairs of an individual; and publication of the matter would or might seriously and prejudicially affect the interests of that body or individual. An example of this would be information that could be considered commercially sensitive.

666. Subsection (5) sets out that this clause applies to reports about the use of technology under clause 69; transparency reports under clause 100; reports about researchers' access to information under clause 101; and reports under this clause.

Chapter 8: Media Literacy

Clause 103: Media Literacy

667. This clause will replace section 11 of the Communications Act 2003, which contains the existing duty on OFCOM to promote media literacy in relation to broadcasting and electronic media. The replacement clause expands and strengthens the existing duty, and applies the duty in relation to online safety.

668. New subsection (1) provides that OFCOM must take action to improve the media literacy of UK users and encourage regulated service providers and broadcasters to use and develop tools which can improve people's digital media literacy. This includes technologies and systems which help users to identify what

type of material they are seeing (for example sponsored content), how reliable and accurate content it is, and how users can control the material they receive.

669. New subsection (3) specifies that in performing its duty, OFCOM must deliver, commission, or encourage education initiatives aimed at improving media literacy rates for UK citizens. This is a new requirement and could include, for example, public awareness campaigns or providing training to improve the skills of teachers.

670. New subsection (4) requires OFCOM to issue guidance on how to evaluate media literacy initiatives and actions. The aim of the guidance is to help improve the quality of evaluations of media literacy initiatives, and to improve overall understanding of what efforts are effective in building long-term media literacy understanding in individuals.

671. New subsection (8) specifies that OFCOM's annual report must contain a summary of the steps that they have taken to fulfil their expanded duty to promote media literacy in relation to the relevant financial year.

Part 5: Appeals and Super-complaints

Chapter 1: Appeals

Clause 104: Appeals against OFCOM decisions relating to the register under section 59

672. This clause allows for appeals against OFCOM's decisions about the inclusion and removal of services from the register of Category 1, Category 2A, and Category 2B services. OFCOM must establish the register and service providers become subject to additional duties with regard to any Category 1, Category 2A, and Category 2B services they provide, by virtue of the service and service provider's inclusion on the relevant part of the register.

673. Subsection (1) allows for appeals to be made in the following circumstances:

a. After OFCOM decides to include a regulated service in the register. This route of appeal may be used when a service is first added to the register, or moved between categories, or when OFCOM reassesses services following the setting of new threshold conditions through regulations.

b. After OFCOM decides not to remove a regulated service from the register (or relevant part of the register). This route of appeal may be used when a service has been on a relevant part of the register, but the provider of that service no longer considers the service to meet the threshold conditions to merit being on the register, or that part of it.

674. Subsection (2) establishes that the route of appeal against such decisions lies by way of an appeal to the Upper Tribunal. It also makes clear that only the provider of a service included on the register can make an appeal.

675. Subsection (3) states that where a provider appeals a decision to be included in the relevant sections of the register, any "special requirements" need not be complied with until the appeal is concluded. Under subsection (4), these "special requirements" are defined as any additional requirements that would be placed on the relevant providers if the service they provided was added to the relevant sections of the register. Note that this only applies to the first type of appeal specified above. Service providers will need to comply with "special requirements" while an appeal against an OFCOM decision not to remove a regulated service from the register (or relevant part of the register) is ongoing.

676. Subsection (5) provides that the Upper Tribunal must decide the appeal on the same principles that apply on an application for judicial review - meaning that the tribunal will assess the legality, fairness and rationality of the decision and the fairness of the procedure used to make it, rather than conducting a review of the merits of a decision.

677. Subsection (6) states that the Upper Tribunal may either dismiss the provider's appeal or quash OFCOM's decision.

678. Should the Tribunal quash the decision then subsection (7) provides that the Tribunal must remit the decision back to OFCOM, with any directions that the Tribunal thinks are appropriate.

Clause 105: Appeals against OFCOM notices

679. This clause establishes routes of appeal against other decisions made by OFCOM; in particular, the decision to give a Use of Technology Notice, a confirmation decision, or penalty notice.

680. Subsection (1) allows a person who is given a Use Of Technology Notice to appeal against OFCOM's decision to issue one against them pursuant to clauses 64, 65 and 67.

681. Subsection (2) allows for any person who has been the subject of an enforcement decision to appeal against OFCOM's decision to issue:

a. confirmation decisions (as set out in clause 83); and

b. penalty notices (as set out in clauses 84, 89 and 90).

In addition, the Upper Tribunal may give permission to other parties who have not been given the confirmation decision or penalty notice to appeal an OFCOM decision, as long as they are judged to have sufficient interest in that original decision: subsection (3). For example, this could be a civil society group rather than the provider themselves.

682. In all of the above cases, appeals would be by way of an appeal to the Upper Tribunal.

683. Subsection (4) states that, again, the Upper Tribunal must decide these appeals applying the same principles as for judicial review - as explained in the notes for clause 104.

684. Subsection (5) states that the Upper Tribunal may either dismiss the appeal or quash OFCOM's decision. Should the Tribunal quash the decision then subsection (6) provides that the Tribunal must remit the decision back to OFCOM for reconsideration, with any directions that the Tribunal thinks are appropriate.

685. Subsection (7) cross-references to the instances when penalty notices might be issued.

Chapter 2: Super-complaints

Clause 106: Power to make super-complaints

686. This clause establishes a super-complaints procedure whereby a body representing the interests of UK users of regulated services, or members of the public can make a super-complaint to OFCOM about any feature of one or more regulated services, or the conduct of one or more providers of such services.

687. Subsection (1) sets out that a super-complaint may be made about any particular feature of one or more regulated services, or the conduct of one or more providers of such services, or a combination of the two where there appears to be or where there is material risk of:

a. causing significant harm to users of the services, members of the public or a particular group of users / members of the public;

b. significantly adversely affecting the rights to freedom of expression to users of the service, members of the public or a particular group of users / members of the public;

c. causing significant unwarranted infringements of privacy to users of the services, members of the public or a particular group of users / members of the public; or

d. otherwise having a significant adverse impact on users of the services, members of the public or a particular group of users / members of the public.

688. Subsection (2) provides that an “eligible entity” can bring such a complaint. OFCOM may only consider a super-complaint that relates to the conduct of a single regulated service or single provider of one or more regulated services, if OFCOM believes that the complaint is of particular importance or it relates to impacts on a particularly large number of people (be they users of that service or members of the public).

689. To be eligible, the entity must meet criteria which will be specified in regulations made by the Secretary of State: see subsection (3). One of the criteria which must be specified in the regulations is that the entity is a body representing the interests of users of regulated services, or members of the public or a particular group of such users or members of the public: see subsection (4). Before making these regulations, the Secretary of State must consult OFCOM and such other persons as the Secretary of State considers appropriate: see subsection (5).

690. Subsection (6) defines conduct as that which includes acts and omissions, and “user” is defined as any UK user.

Clause 107: Super-complaints: procedure

691. Subsection (1) gives the Secretary of State the power to make regulations which would set out the procedural aspects of the complaints made under clause 106.

692. Subsection (2) provides examples of the type of matters that these regulations may include; such as, requiring an eligible entity to provide notification to OFCOM of an intention to make a super-complaint. The regulations may also include the form and manner of such a complaint (including requirements for supporting evidence), how OFCOM must respond to such a complaint, and time limits (or provisions for determining the time limits) for carrying out the relevant steps in relation to a complaint.

693. Subsection (3) sets out the consultation requirements for the above regulation. The Secretary of State must consult OFCOM and any other persons they consider appropriate.

Clause 108: Super-complaints: guidance

694. This clause puts a requirement on OFCOM to produce and publish guidance on super-complaints.

695. As per subsection (1), this guidance, must include:

a. Guidance about the criteria for entities eligible to make such complaints;

b. Guidance about procedural matters relating to such complaints such as the quality or type of evidence required as part of a super-complaint; for example, evidence of harm to users or members of the public and evidence of non-compliance with the relevant duties in the Online Safety Bill; and

c. Guidance about any other aspect of such complaints that OFCOM considers it appropriate to include.

696. Subsection (2) provides a requirement for OFCOM to publish the guidance, including guidance that is revised or replaced.

Part 6: Secretary of State's Functions in Relation to Regulated Services

Strategic Priorities

Clause 109: Statement of strategic priorities

697. This clause introduces a power for the Secretary of State to designate and publish a statement of strategic priorities in relation to online safety matters, and the promotion of media literacy where this is relevant to online safety. The statement will allow the government to set out the overall strategic direction for tackling online harms and respond at a high level to future changes. This power is similar to the existing power the Secretary of State has in the Communications Act 2003 in relation to telecommunications, management of radio spectrum and postal services.

698. Subsection (1) specifies that in order to designate a statement of strategic priorities, the Secretary of State must first consult and follow the parliamentary procedure set out in clause 110.

699. Subsection (3) provides that the statement may specify particular outcomes to deliver the strategic priorities. For example, the Secretary of State may set a target eradication rate for child sexual exploitation and abuse (CSEA) images online or look to reduce regulatory burdens on companies.

700. Subsections (6) to (8) make provision for the amendment of a statement of strategic priorities in whole or in part, by the issuing of a subsequent statement. There are limited circumstances in which amendments may be made within a five year period, including where there has been a significant change in government policy affecting online safety matters.

Clause 110: Consultation and parliamentary procedure

701. This clause sets out the consultation and parliamentary procedure requirements that must be satisfied before the Secretary of State can designate a statement of strategic priorities under clause 109.

702. Subsection (2) states that the Secretary of State must consult OFCOM and other persons the Secretary of State considers appropriate on a draft of the statement. For example, the Secretary of State may wish to consult other government departments, industry bodies, academics, policy institutes/think tanks, or other regulators.

703. Subsection (3) provides for a period of at least 40 days for such consultation with OFCOM, following which the Secretary of State must make any changes to the draft statement that appear necessary to the Secretary of State and then lay the draft statement before Parliament (subsection (4)).

704. Subsection (5) specifies that the Secretary of State must wait for the 40-day period after laying the draft statement to expire before designating it. The statement cannot be designated if either House of Parliament resolves not to approve the draft statement during that 40-day period.

Directions to OFCOM

Clause 111: Secretary of State directions about advisory committees

705. This clause enables the Secretary of State to give OFCOM a direction to establish an expert committee to give advice to OFCOM about the online safety matters which the Secretary of State has specified in the direction.

706. The Secretary of State must consult OFCOM before issuing a direction, and can vary or revoke the direction at any time. For example, this power could be used in a scenario where there is growing concern around the understanding of members of the public on the impact of social media on societal polarisation. It is unlikely that the duty of care alone, which is limited to harm to individuals, would address this issue. In consultation with OFCOM, the Secretary of State could direct OFCOM to establish an advisory committee to facilitate multi-stakeholder dialogue and build a greater understanding of the issue.

707. Subsection (3) sets out that OFCOM must appoint a committee chair, and that the number of members apart from the chair is at OFCOM's discretion, unless the direction specifies otherwise.

708. Subsection (4) places a duty on an advisory committee established under this direction to publish a report within 18 months of it being established, and to report periodically after that, unless the direction specifies otherwise.

Clause 112: Secretary of State directions in special circumstances

709. This clause enables the Secretary of State to give OFCOM directions in circumstances where they consider there is a threat to the health or safety of the public, or to national security. This includes directing OFCOM to prioritise action to respond to such a specific threat when exercising its media literacy functions and to require a service provider to publicly report on what steps it is taking to respond to that threat.

710. Subsection (1) specifies the circumstances under which the Secretary of State is able to issue directions under this clause, where the Secretary of State has reasonable grounds to believe there is a threat to the health or safety of the public, or to national security.

711. Subsection (2) provides that the Secretary of State can direct OFCOM to give priority for a specified period to specified objectives regarding OFCOM's duty to promote media literacy, as set out in section 11 of the Communications Act 2003, in relation to broadcasting and electronic media. This provides the Secretary of State with the option to step in to ensure that OFCOM is taking steps to address threats of disinformation and misinformation.

712. Subsection (3) provides that the Secretary of State can direct OFCOM to issue a public statement notice that requires providers of a regulated service to set

out the steps the provider is taking in response to the threat presented to the health or safety of the public, or to national security.

713. Subsection (6) specifies that the Secretary of State must publish the reasons for giving a direction related to OFCOM's media literacy priorities or to require OFCOM to give a public notice statement to service providers in circumstances where there is a threat to the health or safety of the public. There is an exception to the requirement of publishing the reasons for giving a direction where it relates to a threat to national security, the Secretary of State can vary or revoke a direction at any time. If so, OFCOM can vary or revoke the public statement notice it has given pursuant to the Secretary of State's direction: see subsection (7) and (8).

Guidance

Clause 113: Secretary of State guidance

714. This clause enables the Secretary of State to give guidance to OFCOM relating to OFCOM's exercise of its statutory powers and functions. The guidance will provide clarity to OFCOM and others about how the Secretary of State expects OFCOM to carry out its statutory functions. The Secretary of State must consult OFCOM before issuing new guidance, or revising or replacing guidance: see subsection (3). The Secretary of State must also publish any new, revised or replacement guidance and lay it in Parliament: see subsections (6) and (7).

715. Subsection (1) states that the Secretary of State may give guidance to OFCOM about the exercise of its functions under the Online Safety Bill. The Secretary of State may also give guidance on the exercise of OFCOM's general powers and its media literacy functions under the Communications Act 2003.

716. Subsection (2) exempts guidance to OFCOM about fees and guidance about OFCOM's media literacy functions in relation to services other than regulated services from the definition of 'the guidance', thereby excluding the requirements of subsections (3) to (8) from applying to such guidance.

717. Subsection (4) states that the guidance should not be revised more frequently than every three years, save for if one of the following two exceptions applies:

a. The guidance needs to be amended as a result of a change to the Online Safety Act or to the media literacy provisions in the Communications Act 2003.

b. There is agreement between OFCOM and the Secretary of State that the guidance should be revised or replaced.

718. Subsection (5) requires the guidance to be issued as one document.

719. Subsection (8) sets out OFCOM's responsibilities in relation to the guidance. Namely, OFCOM must have regard to the guidance when exercising any functions to which the guidance relates or when considering whether or not to exercise such functions.

Annual Report

Clause 114: Annual report on the Secretary of State's functions

720. Section 390 of the Communications Act 2003 requires the Secretary of State to prepare and lay before Parliament annual reports about the performance of their functions under specific legislation, including the Communications Act 2003, the Office of Communications Act 2002 and the Broadcasting Acts 1990 and 1996.

721. This clause amends the Communications Act 2003 by adding the functions under this Bill to the list of functions which the Secretary of State must include in their annual report to Parliament.

Review

Clause 115: Review

722. This clause provides for a review to be undertaken by the Secretary of State, published and laid before Parliament, between 2 and 5 years after the duties on services in Part 2 are commenced in order to assess the effectiveness of the regulatory framework. The timing requirement (subclause (2)) is designed to ensure there is adequate time to allow the regime to be in operation before the review takes place, and that a review will take place in a timely manner.

723. Subsection (1) sets the scope of the review to the operation of (a) the regulatory framework under the Online Safety Act and (b) section 11 of the Communications Act 2003 (duty to promote media literacy) to the extent that that section relates to online safety matters.

724. Subsection (3) specifies some of the areas the review must consider in assessing the effectiveness of the regulatory framework. This includes the impact of the systems and processes regulated services have put in place, and whether the regulation of services is proportionate.

725. Subsection (4) specifies further areas that must be considered as part of the review. These are the effectiveness of OFCOM's information gathering, information sharing and enforcement powers; the extent to which OFCOM has had regard to the desirability of encouraging innovation; and whether it would be appropriate for OFCOM to be able to exercise the power to require that a provider name a senior manager in their response to an information notice (clause 71), in light of the effectiveness of OFCOM's power to require information using an information notice (clause 70).

Part 7: General and Final Provisions

Providers of regulated services

Clause 116: 'Provider' of user-to-user service or search service

726. The Online Safety Bill places duties on providers of user-to-user and search services. This clause operates to determine who is the 'provider' of such a service, and therefore who is subject to the duties imposed on providers.

727. For user-to-user services, subsection (2) sets out that the provider is the entity (that is the body or association of persons or organisation (see clause 137(1)) which controls who can use the user-to-user service.

728. Subsection (3) makes it clear that, if use of a service is controlled by an individual (or individuals) rather than an entity, that individual (or those individuals) will be considered the provider of the service.

729. Subsection (4) clarifies that someone who provides an access facility in relation to a user-to-user service, which is a facility that can be withdrawn, adapted or manipulated in order to impede access to the user-to-user service (see clause 93), is not a provider of that service. Examples of "access facilities" would include internet access services, web hosting services, domain name services, security software, content delivery network services, app stores and payment service providers. This subsection therefore establishes and highlights the distinction between the provider of a user-to-user service itself and the provider of any services which enable the regulated service to function.

730. Furthermore, enterprise software, such as software-as-a-service products, also counts as an access facility; therefore, this subsection makes clear that where multiple entities (or individuals) may be involved in the provision of a service to the end user, it is only the entity with control over who can use the service which is to be considered the service provider. For example, if entity A buys software from software company B on a software-as-a-service basis, and the software enables entity A to create a regulated service, entity A (rather than software company B) is to be considered the service provider.

731. Subsections (5) and (6) set out that a provider of a search service is the entity (that is the body or association of persons or organisation (see clause 137)) which controls its operations. If no entity controls the service, but rather an individual or individuals have control over its operations, that individual or those individuals will be considered to be the provider. As set out in subsection (9), the operations of the search service are taken to mean operations which enable users to make search requests, and which subsequently generate responses to those requests.

732. Subsections (7) and (8) state that if a user-to-user service or a search service is generated by a machine (such as an algorithm), then the entity - or, if there is no entity, the individual or individuals - that controls the machine will be the provider of the service.

Clause 117: Providers that are not legal persons

733. Subsection (1) sets out the definition of a "relevant entity", which is a provider of a regulated service that does not have a separate legal existence. A partnership or an unincorporated association (a group that agrees to come together for a specific purpose) would both be examples of bodies which do not have a separate legal existence. On the other hand, a company would have its own separate legal existence, and therefore could not be a relevant entity for the purposes of this clause.

734. Subsection (2) states that penalty notices given to relevant entities are to be paid from the entity's funds. The definition of "penalty notice" for this clause is set out in subsection (6), and comprises: a confirmation decision (clause 83), a penalty notice for failure to comply with various requirements in a confirmation decision (clause 84), a penalty notice for non-payment of a fee (clause 89), and a penalty notice for failure to comply with a use of technology notice (clause 90).

735. Subsection (3) states that notices issued to a relevant entity under Chapter 4 (use of technology), Chapter 5 (information) or Chapter 6 (enforcement) of Part 4 of the Online Safety Bill will continue to have effect regardless of any changes to the entity's membership.

736. Subsection (4) states that when a penalty notice is given jointly to two or more officers or members of a relevant entity (which subsection (5) provides includes employees of the entity or individuals associated with the entity), those individuals are jointly and severally liable to pay the penalty. This means that any of those individuals can be pursued for full payment of the penalty.

Clause 118: Individuals providing regulated services: liability

737. This clause sets out how liability under the Online Safety Bill applies to a group of two or more individuals who together are providers of a regulated service.

738. Subsection (2) sets out that, where a duty or requirement is imposed under Chapters 2, 3 and 4 of Part 2 (duties of care), clause 51 (fees: duty to notify) or clause 52 (duty to pay fees) on a group of two or more individuals who together provide a regulated service, that duty or requirement is to be taken to be imposed on both (or all) of the individuals jointly and severally. This means that any of those individuals can be pursued for full payment of the penalty.

739. Subsection (3) sets out that any notice under Chapter 4 (use of technology), Chapter 5 (information), or Chapter 6 (enforcement) of Part 4 in respect of a regulated service provided by a group of two or more individuals may be either given to one individual, or jointly to two or more of the individuals.

740. Subsection (4) provides that, where a penalty notice is given jointly to two or more individuals, those individuals are jointly and severally liable to pay the penalty contained in that notice. As noted above, this means that any of those individuals can be pursued for full payment of the penalty.

741. Subsection (5) explains that penalty notices under this clause are confirmation decisions that impose a penalty (clause 83), penalty notices for failure to comply with various requirements in a confirmation decision (clause 84), penalty notices for non-payment of a fee (clause 89), and penalty notices for failure to comply with a use of technology notice (clause 90).

Clause 119: Liability of parent entities for failures by subsidiary entities

742. This clause explains how parent entities can be liable for failures of their subsidiary entities to comply with various duties and requirements imposed on them by the Online Safety Bill.

743. Subsection (1) makes clear that in order for subsection (2) to apply OFCOM must first have grounds to issue the subsidiary entity ("E") with a relevant decision or notice in respect of a regulated service which E provides, and E must have a parent undertaking. The list of relevant decisions and notices are set out in subsection (8), and comprise: a confirmation decision (clause 83), a penalty notice for failure to comply with various requirements in a confirmation decision (clause 84), a penalty notice for non-payment of a fee (clause 89), or a penalty notice for failure to comply with a use of technology notice (clause 90).

744. Once the conditions in subsection (1) are met, subsection (2) provides that a relevant decision or notice may be given only to E or jointly to both E and the parent undertaking. However, subsection (3) provides that, before such a decision or notice can be issued to the parent undertaking, the parent undertaking must have been given an opportunity to make representations to OFCOM.

745. Subsection (4) sets out that if a decision or notice is given to both E and the parent undertaking, then both entities are jointly and severally liable to comply with the requirements, or pay the penalty imposed on them. As set out in subsection (5), an entity will be a parent undertaking' in relation to E if the entity satisfies the circumstances in section 1162(2)(b), (2)(c), (2)(d) or (4) of the Companies Act 2006 in relation to E. These provisions in the Companies Act concern circumstances demonstrating the level of control the parent entity has over the subsidiary entity.

746. In order to determine whether the circumstances in the relevant Companies Act provisions exist, subsection (6) sets out how paragraph 4 of Schedule 7 to the Companies Act 2006 it is to be read in order for a parent undertaking to be deemed to have the right to exercise a dominant influence over E. It must be the case that the parent undertaking has the right to give directions with respect to E's policies relating to compliance with the Online Safety Bill's regulatory requirements, which E's directors are obliged to comply with.

747. Subsection (7) provides that, for the purposes of this clause, section 1162 (meaning of parent and subsidiary undertaking) and Schedule 7 of the Companies Act 2006 apply to an entity which is not deemed to be an undertaking as if they were an undertaking. These provisions are also to be read with any necessary modification so that they can apply to an entity formed under the law of a country outside of the UK.

Clause 120: Liability of controlling individuals for failures by entities

748. This clause explains the circumstances under which a controlling individual can be found liable for the failure of an entity to adhere to duties or requirements under the Online Safety Bill.

749. Subsection (2) provides that a relevant decision or notice may be given solely to an entity ("E"), or jointly to E and to the individual or individuals who control E if the conditions in subsection (1) are met. The conditions in subsection (1) are that (i) OFCOM is satisfied that there are grounds to give E a relevant decision or notice, (ii) E is the provider of that regulated service, and (iii) an individual(s) controls E. The decision or notice may not be given to that individual(s) unless they have had the opportunity to make representations to OFCOM (subsection (3)).

750. The list of relevant decisions and notices is set out in subsection (8): a confirmation decision (clause 83), a penalty notice for failure to comply with various requirements in a confirmation decision (clause 84), a penalty notice for non-payment of a fee (clause 89), or a penalty notice for failure to comply with a use of technology notice (clause 90).

751. Subsection (4) provides that, if a relevant decision or notice is given jointly to E and to an individual(s), they are jointly and severally liable to comply with the requirements set out in the decision or notice, and/or (if one is stipulated) to pay the penalty imposed on them.

752. Subsection (5) sets out, for the purposes of this clause, when an individual(s) would be deemed to control E. An individual or individuals will be deemed to be in control of E where, if they were an undertaking, they would be considered to be a parent undertaking within the meaning of section 1162 of the Companies Act 2006, because they meet the conditions in subsections (2)(b), (2)(c) or (2)(d) or (4)(a) of that section. The relevant conditions in subsection (2) are that (i) the individual(s) is a member of E and has the right to appoint or remove a majority of the E's board of directors, or (ii) has a right to exercise a dominant influence over E (by virtue of provisions in E's articles or a control contract), or (iii) controls a majority of the voting rights in E. The relevant condition in subsection (4)(a) is that the individual(s) has the right to exercise, or actually exercises, dominant influence or control over E.

753. Subsection (6) specifies how paragraph 4 to Schedule 7 of the Companies Act 2006 is to be applied to this section. The result of this subsection is that, when considering whether an individual exercises a dominant influence over E by virtue of provisions in E's articles or a control contract, the individual should not be regarded as having a dominant influence unless they have the right to give directions with respect to policies related to compliance with the regulatory requirements imposed by this Bill, and E's directors are obliged to comply with these directions. This does not apply when considering section 1162(4)(a) of the Companies Act 2006 (paragraph (4)(3) of Schedule 7 to the Companies Act 2006).

754. Subsection (7) provides that, for the purposes of this section, section 1162 (parent and subsidiary undertaking) and Schedule 7 of the Companies Act 2006 apply to an entity which is not deemed to be an undertaking as if they were an

undertaking. These provisions are also to be read with any necessary modification so that they can apply to an entity formed under the law of a country outside of the UK.

Clause 121: Liability of subsidiary entities for failures by parent or fellow subsidiary entities

755. This clause explains how a subsidiary entity can be found liable for failures of their parent entity or another subsidiary entity to adhere to duties or requirements under the Online Safety Bill.

756. Subsections (1) and (2) provide that, in a scenario where OFCOM is satisfied that there are grounds to give an entity ("E") a relevant decision or notice in relation to a regulated service provided by E, and E is a parent undertaking in relation to another undertaking (the subsidiary undertaking), OFCOM may either give said decision or notice only to E or to both E and the subsidiary undertaking.

757. Subsection (3) provides, however, that OFCOM will only be able to issue the decision or notice to both E and the subsidiary undertaking where the subsidiary undertaking has contributed to the failure dealt with by the decision or notice. The subsidiary undertaking must also have been given the opportunity to make representations to OFCOM.

758. Subsections (4) and (5) provide that, in a scenario where OFCOM have grounds to give E a relevant decision or notice relating to a regulated service provided by E, and E is a subsidiary undertaking with one or more fellow subsidiary undertakings, the relevant decision or note may be given only to E or jointly to E and a fellow subsidiary undertaking.

759. Subsection (6) makes it clear that OFCOM will only be able to issue the decision or notice to both E and a fellow subsidiary undertaking where the fellow subsidiary undertaking has contributed to the failure dealt with by the decision or notice. The fellow subsidiary undertaking must also have been given the opportunity to make representations to OFCOM.

760. Subsection (7) sets out that if a decision or notice is given to both E and a fellow subsidiary undertaking, then both entities will be jointly and severally liable to comply, or pay the penalty imposed on them.

761. Subsection (8) provides that the terms 'fellow subsidiary undertaking', parent undertaking' and 'subsidiary undertaking' have the meaning given in sections 1161(4) and 1162 of the Companies Act. The list of relevant decisions and notices are set out in subsection (8), and comprise: a confirmation decision (clause 83), a penalty notice for failure to comply with various requirements in a confirmation decision (clause 84), a penalty notice for non-payment of a fee (clause 89), or a penalty notice for failure to comply with a use of technology notice (clause 90).

762. Subsection (9)(a) provides that the definition of undertakings in section 1161(1) of the Companies Act 2006 for the purpose of this clause of the Bill is to apply in relation to an entity which is not an undertaking under that definition as if they were an undertaking. Subsection (9)(b) also allows for sections 1161(4) and 1162 of, and Schedule 7 to, the Companies Act 2008 to be read with any necessary

modifications required for entities that were formed under the law of a country outside the UK.

Clause 122: “User” and “United Kingdom user” of service

763. This clause clarifies the term “United Kingdom user”, and also makes provision in relation to the term “user” of an internet service, user-to-user service or search service.

764. Subsection (1) states that a “United Kingdom user” covers an individual who is in the United Kingdom, or an entity which is incorporated or formed under the law in any part of the United Kingdom.

765. Subsections (2) makes clear that a person using a service counts as a “user” whether or not they are registered with that service.

766. Subsection (3) outlines the circumstances where someone would not be counted as a user. Specifically, the following would not count as users when acting in the course of the provider’s business: individuals (where they are also the service provider); officers of an entity (where that entity is the service provider); persons who work for the provider; and anyone else providing a business service to the service provider.

767. Subsection (4) defines “acting in the course of the provider’s business”. It makes clear that an employee of Retailer X, which provided regulated Service A, would not count as a user if uploading content to Service A in the course of their employment by Retailer X, although they would count as a user of Service A if uploading content to Service A in a personal capacity.

Clause 123: Information offences: supplementary

768. This clause sets out further detail on the offences of failing to comply with requirements in an information notice (under clause 72) and on the liability of named senior managers in connection with such an offence (under clause 73).

769. Subsection (1) confirms that proceedings for an offence in connection with a failure by a person to comply with requirements in an information notice may be brought only if:

a. the person has received a provisional notice of enforcement action;

b. they have received a confirmation decision in respect of that failure, and they have not complied with the requirements of the original information notice by a deadline set within the confirmation decision;

c. a penalty has not been imposed by OFCOM in respect of that failure; and

d. neither a service restriction order nor an access restriction order has been made in respect of that failure.

770. Subsection (2) confirms that, if any proceedings are to be brought against a senior manager for the offence of failing to prevent an offence of failing to comply

with an information notice, the conditions set out in subsection (1) must also be met in relation to the alleged failure to comply with an information notice.

771. Subsection (3) provides that, where a penalty is imposed on a person, that person may not at any time be convicted of an offence of failing to comply with an information notice under clause 72, in respect of the act or omission that resulted in the penalty. Subsection (4) similarly provides that a senior manager of an entity may not at any time be convicted of an offence under clause 73 of failing to prevent that entity failing to comply with an information notice if a penalty has already been imposed on the entity in respect of its failure to comply with an information notice.

772. Subsection (5) set out that, for the purpose of this clause, 'penalty' refers to a penalty imposed by a confirmation decision under clause 83(6) or by a penalty notice under clause 84(3).

Clause 124: Defences

773. This clause applies where a person relies on a defence under clause 72 or 73.

774. If evidence is provided which is sufficient to raise an issue with respect to the defence, there is a presumption that the defence has been established unless the prosecution can prove beyond any reasonable doubt that it is not.

Clause 125: Liability of corporate officers for information offences

775. This clause sets out the instances where officers of relevant entities may be liable for information offences committed by that entity.

776. Subsection (1) defines the term 'relevant entity' for the purpose of this clause. It provides that a relevant entity is an entity which is both a provider of a regulated service and a legal person under the law under which it is formed.

777. Subsection (2) provides that, if an offence of failing to comply with an information notice is committed by a relevant entity and that offence is proved to have been committed with the consent or connivance of, or is attributable to the neglect of an officer, both the officer and the relevant entity will be guilty of the offence. So long as the requirements in clause 123(1) are complied with, both the officer and the relevant entity are liable to criminal proceedings and sanctions.

778. Subsection (3) sets out that, where an entity is a body corporate, an 'officer' is a person occupying the position of a director, manager, secretary or other similar officer, regardless of their formal job title; or a person claiming to act in such capacity. Subsection (5) confirms that, where the affairs of a body corporate are managed by the members, a member is guilty of an offence of failing to comply with an information notice and liable to criminal proceedings if a failure by the body corporate to comply with an information notice is committed with the consent or connivance of, or is attributable to the neglect of, that member in performing their management functions. This offence is different in nature from the named senior manager offence set out in section 73. Criminal liability for consent or connivance is a different kind of

liability, entirely contingent on the offence committed by the entity, whereas the named senior managers' offence under section 73 is an offence in its own right.

779. Subsection (4) sets out that, where the relevant entity is a partnership and is not a body corporate, an 'officer' is a partner or someone purporting to act as such.

780. For both subsections (3) and (4), the term 'body corporate' includes an entity that is incorporated outside of the United Kingdom (subsection (6)).

Clause 126: Application of information offences to providers that are not legal persons

781. This clause sets how information offences apply to providers that are not legal persons. The definition of 'relevant entity' for the purposes of this clause is set out in subsection (1) and means an entity which is a provider of a regulated service that does not have a legal personality under the law under which it is formed. Under English and Welsh law, a partnership and an unincorporated association (a group that agrees to come together for a specific purpose) would both be examples of entities which do not have a legal personality.

782. Subsection (2) specifies that proceedings for an offence (under clause 72) alleged to have been committed by the relevant entity must be brought against the entity in its own name. It must not be bought in the name of any of its officers, members or partners.

783. Subsection (3) states that, for such proceedings, the rules of court relating to service of documents have the same effect as if the entity were a body corporate (e.g. a company), and that the listed provisions in subsection (3)(b) also apply as they would apply in relation to a body corporate.

784. Subsection (4) states that a fine imposed on a relevant entity under clause 72 is to be paid out of the entity's funds.

785. Subsection (5) provides that, if the relevant entity commits the offence of failing to comply with an information notice, and this offence was committed with the consent or connivance of, or can be attributed to, the neglect of an officer, then the officer is also guilty of this offence. The officer is thus liable to be proceeded against and punished accordingly, subject to clause 123(1). Subsection (8) provides that subsection (2) does not prejudice the liability of an officer under subsection (5).

786. Subsections (6) and (7) define what is meant by 'officer' in relation to a partnership or a relevant entity other than a partnership.

Clause 127: Extra-territorial application

787. This clause specifies that references to regulated services and OFCOM information-gathering powers apply to services provided from outside the UK (as well as to services provided from within the UK).

788. Subsection (1) states that the scope of the Bill extends to internet services, user-to-user services, and search services provided from outside the United Kingdom.

789. Subsection (2) specifies that OFCOM's information-gathering powers under clause 70 extend to requiring the production of documents held outside the United Kingdom.

790. Subsection (3) states that OFCOM's power to request interviews under clause 76 extends to requiring the attendance of individuals who are outside the United Kingdom.

Clause 128: Information offences: extra-territorial application and jurisdiction

791. This clause outlines that information offences apply to acts done in the United Kingdom or elsewhere, and specifies how proceedings should be taken where acts take place outside the United Kingdom.

792. Subsection (1) states that the offence in clause 72 applies to acts done in the United Kingdom or elsewhere by a provider of a regulated service.

793. Subsection (2) states that the offence in clause 73 applies to acts done in the United Kingdom or elsewhere by an individual.

794. Subsection (3) states that the offences in clauses 125(2) and 126(5) apply to acts done in the United Kingdom or elsewhere by an individual.

795. Subsection (4) states that if an offence is committed under clause 72 or 73 outside the United Kingdom, proceedings may be taken at any place within the United Kingdom, and the offence can be treated as having been committed at that place within the United Kingdom. Subsection (5) details the courts at which such legal action may be brought if the proceedings are to take place in Scotland.

796. Subsections (6) sets out definitions applicable to this clause.

Clause 129: Service of notices

797. This clause sets out the process for issuing notices relating to transparency reports, use of technology notices, information notices, enforcement notices and public statement notices to providers of regulated services both within, and outside of the UK.

798. Subsections (2) and (6) provide that OFCOM can issue notices to a provider of a regulated service by handing it to the relevant person, leaving it at or posting it to any address where OFCOM have reasonable grounds to believe that the notice will come to the attention of the relevant person, or by emailing it to the relevant person's email address. By virtue of subsection (9) a person's email address is that which they have published as the address to be contacted at or where there is no such address, any email address OFCOM reasonably believe that the notice will come to the relevant person's attention. A notice sent by email is taken to have been given to that person 48 hours after it is sent: see subsection (10).

799. Subsections (2) and (7) provide that OFCOM can give notice to a person who is not a provider of a regulated service by handing it to the relevant person; where the person is an entity, leaving it at or posting it to the entity's registered or principal

office; where the person is not an entity, leaving it at or posting it to the person's last known address; or sending it by email to the person's email address. Subsection (8) states that, for entities which are registered, carrying on business, or with offices outside the UK, its principal office includes its principal office in the UK or, should the entity not have an office in the UK, any place within the UK at which OFCOM reasonably believes the notice will come to the attention of a director or other officer.

800. Subsection (3) provides that, in the case of a company or other body corporate, the relevant person to give notice to is any officer of that body. Subsection (11) notes that, in this section, an officer includes a director (which is anyone who has the role of a director, regardless of what they are called), a manager, a secretary and a member, if the entity's day to day affairs are controlled by its members.

801. Subsection (4) states that, for a partnership, the relevant person to give notice to is either a partner or a person with control and management of the partnership.

802. Subsection (5) provides that for bodies which do not have a separate legal existence, save for in the case of partnerships, the relevant person who should be given notice is any member of the entity's governing body. This subsection would apply, for example, to an unincorporated association (a group that agrees to come together for a specific purpose) but not to a company, as companies enjoy a legal existence separate to that of their directors or shareholders.

Clause 130: Repeal of Part 4B of the Communications Act 2003

803. This deletes clauses pertaining to the regulation of video sharing platform services from the Communications Act 2003 and the Audiovisual Media Services Regulations 2020.

Clause 131: Repeals: Digital Economy Act 2017

804. This clause deletes Part 3 of the Digital Economy Act 2017 (which makes provision in relation to online pornography and an age verification system) and removes the obligation for the Secretary of State to issue a code of practice for providers of online social media platforms by deleting section 103 of that Act.

Clause 132: Regulations

805. This clause sets out how the powers to make regulations conferred on the Secretary of State and the Scottish Ministers will be used in practice.

806. As set out in subsection (1), regulations under this Act may make different provisions for different purposes, with regard to both user-to-user services and search services and to different types of services within these groups.

807. Subsection (2) explains that any regulations made using powers granted to the Secretary of State by the Online Safety Bill must be made by statutory instrument.

808. These regulations must be made using the affirmative resolution procedure, where they relate to the following:

a. Exempting low-risk user-to-user or search services;

b. Varying the online safety objectives;

c. Repealing the exemption for comments and reviews on provider content;

d. Defining terrorism offences;

e. Defining child sexual exploitation and abuse (CSEA) offences;

f. Defining ‘qualifying worldwide revenue’ and ‘qualifying period’ for the purpose of fees;

g. Defining ‘qualifying worldwide revenue’ for the purpose of penalties;

h. Defining which entities are eligible to make a super-complaint

Under the affirmative resolution procedure the regulations must receive explicit approval from both Houses of Parliament before becoming law.

809. These regulations should generally be made using the negative procedure where they relate to the following:

a. Meaning of “illegal content”;

b. Meaning of “content that is harmful to children”;

c. Meaning of “content that is harmful to adults”;

d. Transparency reports by service providers;

e. Procedural matters relating to super-complaints;

f. Threshold conditions for categories of regulated services.

Under the negative resolution procedure the regulations will be made (become law) and be laid before Parliament, and will remain law unless Parliament votes to annul them.

810. However, the first versions of regulations relating to the meaning of illegal content, content that is harmful to children and content that is harmful to adults must be made using the affirmative resolution procedure, and any subsequent versions of these regulations should be made using the negative resolution procedure.

811. Subsection (7) explains that the Scottish Ministers must follow the affirmative procedure in exercising their power to make regulations under clause 43(3).

Clause 133: Meaning of “internet service”

812. This clause sets out the meaning of the term “internet service”.

813. Subsection (2) specifies that services made available by means of the internet and by an electronic communications service count as internet services. For

example, a service which is partly made available over the internet and partly by routing through the public switched telephone network would count as an internet service.

814. Subsection (3) provides that the term “electronic communications service” has the same meaning as in section 32(2) of the Communications Act 2003. As amended by the Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020 (SI 2020/1419), that provision defines “electronic communications service” as a service of any of the specified types provided by means of an electronic communications network, except so far as it is a content service. The specified types of service are: (a) an internet access service (i.e. a service that provides access to the internet and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used); (b) a number-based interpersonal communications service; and (c) any other service consisting in, or having as its principal feature, the conveyance of signals, such as a transmission service used for machine-to-machine services or for broadcasting.

Clause 134: Meaning of terms relating to search services

815. This clause sets-out the meaning of “search engine”.

816. Subsection (2a) defines a search engine as including services or functionalities which allow a user to search some websites or databases, as well as services which allow a user to hypothetically search *all* websites or databases. This differentiation ensures that search engines and vertical search engines are both in regulatory scope. A vertical search engine is a search engine that is only focussed on a specific topic or a genre of content, such as a search engine that only indexes academic articles. Subsection (2b) clarifies that the definition does not include services where a user can only search one website or database, thereby preventing internal website search engines from being in regulatory scope.

817. Subsection (3) describes that a ‘search’ can be initiated by any means, including the input of text, images or speech. This is designed to capture the variety of different ways in which search engines can be operated, including speech based virtual assistants such as Apple’s ‘Siri’ or Amazon’s ‘Alexa’.

818. Subsection (4) defines “search results”, while subsection (5) clarifies that this definition does not extend to paid-for advertisements as set-out in clause 39 (7).

819. Subsection (6) states what is meant by references in the Bill to encountering content “via search results.” Paragraph (b) makes clear that this term does not cover any content encountered by a user on another service which is not presented to that user in response to a search request.

820. Subsection (7) defines “interested person” in relation to a search service.

Clause 135: Meaning of “functionality”

821. This clause sets out the meaning of the term ‘functionality’.

822. Subsection (1) provides that, for user-to-user services, functionality refers to service features which enable interactions between users, including features which enable a user to do anything listed in subsection (2), such as creating a user profile or sending direct messages to other service users. The list in subsection (2) is not an exhaustive list of functionalities which may be found on regulated user-to-user services. The examples included in subsection (2) are self-explanatory.

823. Subsection (3) indicates that, for search services, a search feature would be a clear example of a functionality.

Clause 136: Meaning of “online safety functions” and “online safety matters”

824. This clause sets out the meaning of “online safety functions” and “online safety matters”.

825. Subsection (1) sets out that “online safety functions’’ refers to OFCOM’s functions under this Bill and under sections 3, 7, 11, 14(6)(a) and 14(6B) of the Communications Act 2003. “Online safety functions’’ also covers OFCOM's power to do anything incidental or conducive to carrying out these functions.

826. Subsection (2) provides that “online safety matters’’ means the matters to which OFCOM’s online safety functions relate.

Clause 137: Interpretation

827. Subsection (1) sets out the meanings of various terms used in the Online Safety Bill.

828. Subsection (2) explains what is meant by references in the Bill to “taking down” content.

829. Subsection (3)(a) provides that references in the Bill to use of a service or access to content, also refers to services or content which require payment of a fee, subscription or registration to use or access them.

830. Subsection (3)(b) provides that references in the Bill to the making available, accessing, encountering or sharing of content, includes scenarios where content is only made available, accessed, encountered or shared for a limited period of time.

Clause 138: Index of defined expressions

831. This clause lists those provisions which define or explain terms used in this legislation.

Final provisions

Clause 139: Extent

832. This clause provides that the Bill extends to England and Wales, Scotland and Northern Ireland.

Clause 140: Commencement

833. This clause explains when the provisions of the Bill will come into force.

834. Subsection (1) provides for the commencement at Royal Assent of framework provisions (including the definitions and interpretation clauses) and certain regulation making powers which are needed in advance of the rest of the Act coming into force.

835. Subsection (2) provides that the remaining provisions in the Bill will come into force on such day as the Secretary of State may appoint in regulations. Subsection (3) states that the remaining provisions can be brought into force on different days.

836. Subsection (4) provides that clauses 71 (the requirement to name a senior manager) and 73 (senior management liability: information offences) cannot be brought into force before the publication of the report on the outcome of the review required in clause 115 (Secretary of State's review).

837. Subsection (5) states that the Secretary of State can, through regulations, make transitional or saving provisions in connection with the coming into force of any of the provisions in this Bill.

838. Subsection (6) confirms that any power to make regulations, as set out above, is to be exercised by statutory instrument.

Clause 141: Short title

839. This clause establishes the short title of the Bill as the Online Safety Act 2021.

Financial implications of the Bill

840. The Bill includes powers to allow OFCOM to charge fees to industry in order to become cost neutral to the exchequer. Operating costs incurred by OFCOM in carrying out its functions as Online Harms regulator will be met by proportionate fees charged to industry. Further details of the costs and benefits of provisions are set out in the impact assessment published alongside the Bill.

Compatibility with the European Convention on Human Rights

841. The government considers that the Bill is compatible with the European Convention on Human Rights. Accordingly, a statement under section 19(1)(a) of the Human Rights Act 1998 will be made to this effect.

842. In addition to tackling illegal and harmful content online this legislation will protect freedom of expression and uphold media freedom. Specific provisions have also been included in the Bill to ensure that user's rights to freedom of expression and privacy are considered and protected by providers of regulated services.

Related documents

843. The following documents are relevant to the Bill:

- Online Harms White Paper and Consultation
- Online Hams White Paper Initial Government Response
- Online Harms White Paper Full Government Response
- Impact assessment
- Delegated powers memorandum

Annex A – Glossary

Category 1 services	User-to-user services which meet the Category 1 threshold conditions and are included in the relevant OFCOM register. The providers of these services are subject to additional duties in relation to content that is harmful to adults, content of democratic importance and journalistic content; additional reporting and redress duties; and additional duties with regard to protecting users' freedom of expression and privacy rights. Providers of Category 1 services are also under a duty to produce annual transparency reports
Category 2A services	Search services which meet the Category 2A threshold conditions and are included in the relevant OFCOM register. The providers of these services are under a duty to produce annual transparency reports
Category 2B services	User-to-user services which meet the Category 2B threshold conditions and are included in the relevant OFCOM register. The providers of these services are under a duty to produce annual transparency reports
Code of Practice	A code of practice issued by OFCOM outlines the recommended steps to be taken by providers of services in complying with their duties
Regulated Service	A user-to-user service or search service which is subject to duties under the Bill
Provider	The entity which has control over who may use a service
Service	This may refer to a user-to-user service (an internet service which allows user-generated content to be uploaded or shared by a user), a search service (an internet service which includes a search engine which allows multiple

	websites to be searched), or an internet service (a service made available by means of the internet).

Annex B - Territorial extent and application in the United Kingdom

Provision	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?	Would corresponding provision be within the competence of the National Assembly for Wales?	Would corresponding provision be within the competence of the Scottish Parliament?	Would corresponding provision be within the competence of the Northern Ireland Assembly?	Legislative Consent Motion needed?
Part 1: Overview and key definitions								
Clauses 1-3	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 2: Providers of regulated services: duty of care								
Chapter 1: Introduction								
Clause 4	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 2: Providers of user-to-user services: duty of care								
Clauses 5 - 16	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 3: Providers of search services: duty of care								
Clauses 17-25	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 4: Assessment about access by children								
Clauses 26-28	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 5: Codes of practice								
Clauses 29-38	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 6: Interpretation of Part 2								
Clauses 39-48	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 3: Other duties of service providers								
Chapter 1: Transparency reports								
Clauses 49-50	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 2: Fees								

Provision	Extends to E & W and applies to England?	Extends to E & W and applies to Wales?	Extends and applies to Scotland?	Extends and applies to Northern Ireland?	Would corresponding provision be within the competence of the National Assembly for Wales?	Would corresponding provision be within the competence of the Scottish Parliament?	Would corresponding provision be within the competence of the Northern Ireland Assembly?	Legislative Consent Motion needed?
Clauses 51-55	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 4: OFCOM's powers and duties in relation to regulated services								
Chapter 1: General Duties								
Clauses 56-58	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 2: Register of categories of services								
Clauses 59-60	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 3: Risk assessments								
Clauses 61-62	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 4: Use of technology in relation to terrorism content and children sexual exploitation and abuse content								
Clauses 63-69	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 5: Information								
Clauses 70-79	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 6: Enforcement Powers								
Clauses 80-97	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 7: Committees, research and reports								
Clauses 98-102	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 8: Media literacy								
Clause 103	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 5: Appeals and super-complaints								
Provision	**Extends to E &**	**Extends to E &**	**Extends and**	**Extends and**	**Would correspondin**	**Would correspondi**	**Would correspondi**	**Legislative Consent**

	W and applies to England?	W and applies to Wales?	applies to Scotland?	applies to Northern Ireland?	g provision be within the competence of the National Assembly for Wales?	ng provision be within the competence of the Scottish Parliament?	ng provision be within the competence of the Northern Ireland Assembly?	Motion needed?
Chapter 1: Appeals								
Clauses 104-105	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Chapter 2: Super-complaints								
Clauses 106-108	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 6: Secretary of State's functions in relation to regulated services								
Clauses 109-115	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Part 7: General and final provisions								
Clauses 116-141	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedules								
Schedule 1	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 2	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 3	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 4	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No
Schedule 5	Yes	Yes	Yes	Yes	N/A	N/A	N/A	No

Subject matter and legislative competence of devolved legislatures

1. All provisions of the Bill apply across England, Wales, Scotland and Northern Ireland.

2. The matters to which the provisions of the Bill relate are not within the legislative competence of the devolved administrations.

ONLINE SAFETY BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Online Safety Bill as published in Draft on 12 May 2021 (Bill CP 405).

Ordered by the Department to be printed, 12 May 2021

PUBLISHED BY AUTHORITY OF THE DEPARTMENT

Bill CP 405-EN

ISBN 978-1-5286-2563-0
CCS0421458742